



Erasmus+

Project funded by: **Erasmus+ / Key Action 2**

- Cooperation for innovation and the exchange of good practices, Strategic Partnerships for youth

(European Commission, EACEA)



## E-MANUAL

# FOR YOUNG ENTREPRENEURS

Financed by the European Union. The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors and the Commission cannot be held responsible for any use which may be made of the information contained therein.

## Welcome note

Dear young entrepreneur,

Welcome to the DiFens e-Manual!

Below, you will find information, examples, tips and advice on how to support the work of your business in the digital era. Experts in their fields have compiled it in five sections to be short, to the point, and useful for you, helping you focus on five main areas, related to digital security of any business:

In **Section 1**, you will find some introductory, but also in-depth instructional notes on what business digitalization is, how and where to implement it, why and which tools can help you along the way.

In **Section 2** awaits information on social innovations, social entrepreneurship, the benefits and advantages of social enterprises, as well as the specific threats and opportunities, which arise in that sphere of business.

**Section 3** points your attention to the legal aspects of digitally securing your business, more specifically addressing the questions of data protection, consumer protection, e-commerce and cookies.

**Section 4 and 5** address cybersecurity threats, explaining what they are and how to deal with them, outlining a complete strategy with which you can work.

Every section includes similar parts – in different points, the sections give you information, examples, tips. Aside from that, there is a **checklist** on the topic, to help you check the health of your business against this new information, **recommendations for further reading**, which you can take on if you need more knowledge on the topic, and a **terminology glossary**, which you can always open to and address when the flow is too fast.

## Table of contents

Welcome note.....	2
<b>SECTION I BUSINESS DIGITALIZATION.....</b>	<b>5</b>
A. Introduction.....	8
B. Cloud-based solutions – Functionalities and Threats .....	18
C. Utilization of big data – Opportunities and Threats .....	27
D. Improving Digital Skills of Employees.....	31
E. Business Digitalization Checklist.....	39
F. Terminology glossary .....	42
G. Conclusions and Further Reading .....	43
H. References .....	45
<b>SECTION II DIGITAL SECURITY FOR YOUNG SOCIAL INNOVATORS .....</b>	<b>48</b>
A. Introduction.....	50
B. Social Entrepreneurship in the Digital Era .....	51
C. Digital Implementation of the Social Entrepreneurship Concept.....	56
D. Digital Threats and Opportunities for Social Enterprises .....	58
E. Digital Security Checklist .....	60
F. Terminology glossary .....	61
G. Conclusions and Further Reading .....	63
H. References .....	65
<b>SECTION III LEGAL ISSUES REGARDING DIGITAL SECURITY .....</b>	<b>67</b>
A. Introduction.....	69
B. Data Protection Guidelines.....	70
C. Consumer Protection Guidelines.....	78
D. e-Commerce Guidelines.....	85

E. Cookies .....	89
F. Legal Compliance Checklist .....	93
G. Terminology glossary .....	95
H. Conclusions and Further Reading .....	96
I. References .....	97
<b>SECTION IV CYBERSECURITY .....</b>	<b>98</b>
A. Introduction.....	99
B. Digital Security as a Technical Problem .....	102
C. Impact of Digital Security Breaches on Business Environment Processes	122
D. Cybersecurity Solutions.....	125
E. Cybersecurity Checklist.....	130
F. Terminology glossary .....	132
G. Conclusions.....	134
H. References .....	135
<b>SECTION V DIGITAL SECURITY RISK ASSESSMENT .....</b>	<b>138</b>
A. Introduction.....	140
B. Digital security as a Technical Risk .....	143
C. Digital Security as an Economic Risk .....	153
D. Integrating Digital Security as part of an organisation's overall Risk Management and Decision-Making Processes .....	155
E. Digital Security Risk Assessment Checklist.....	162
F. Terminology glossary .....	164
G. Conclusions and Further Reading .....	165
H. References .....	166
<b>Thank you from the DiFens team .....</b>	<b>169</b>

# **SECTION I**

**BUSINESS DIGITALIZATION**

## List of abbreviations

Abbreviation	Definition
CEO	Chief Executive Officer
IoT	Internet of Things
BI	Business Intelligence
ROI	Return on Investment
CRM	Customer Relationship Management
IT	Information Technologies
URL	Uniform Resource Locator
CIO	Chief Information Officer
GPS	Global Positioning System
QR code	Quick Response Code
ERP	Enterprise Resource Planning
SQL	Structured Query Language
DAP	Digital Adoption Platform
POS	Point of sale
SLA	Service Level Agreement
AI	Artificial Intelligence
APIs	Application Interfaces
OWASP	Open Web Application Security Project

CA	Computer Associate
USB	Universal Serial Bus
SMEs	Small and Medium-sized Enterprises
RFID	Radio Frequency Identification
HR	Human Resources
ICT	Information and Communication Technology



## A. Introduction

### **Business in face of the Digital Era**

The world has gotten more interconnected than ever. The opportunity to plunge into a high-octane, high-volume and ever-changing reality starts to transform into a necessity, for entrepreneurial schemes and entrepreneurs alike. The penetration of technology into the business world is in question no more. The main characteristics to be examined are the imminent alteration of the nature of business itself, which is only exacerbated by the work habits of Millennials. Among the main pillars of Business Digitalization, many of those needs are to be addressed.

Any modern business is well advised to balance growth, risk taking, and humans accordingly. Should growth become efficient, sky-rocketing, much like any “unicorn” start-up under the sun, will become a possible scenario. Incorporating technology to increase productivity and safeguarding one’s business by planning ahead, minimize risk. On the other end of the spectrum, there are the customers and the employees. Ease of access meets productivity when a business adopts new technologies and the quality of life improvements that they carry.

### **Being competitive**

Edge. Living, working, and doing business on the edge, in harmony with planning far beyond the prescribed horizons, keep one agile. Creating a competitive advantage and pursuing this purpose to the limits is one strategy that illustrates the sum of many an action. The steppingstone is a solid positioning from day one. Standing out of the crowd as an authority, expert and leader can make a world of difference while the company grows. The digital era calls for a deep-dyed revolution.

That said, there is no need to reinvent the wheel. Following a clear mission that reflects the needs of the ever-changing market is key. A constant analysis of the competition and the customers can enable a business to stay focused. Customer development is a real need. On top of that, developing the people behind the scenes, inspiring and leading them, stands on an equally high pillar. Being innovative through

and through, aids an entrepreneur in advancing safely on all the aforementioned sectors.

### **The need to adapt**

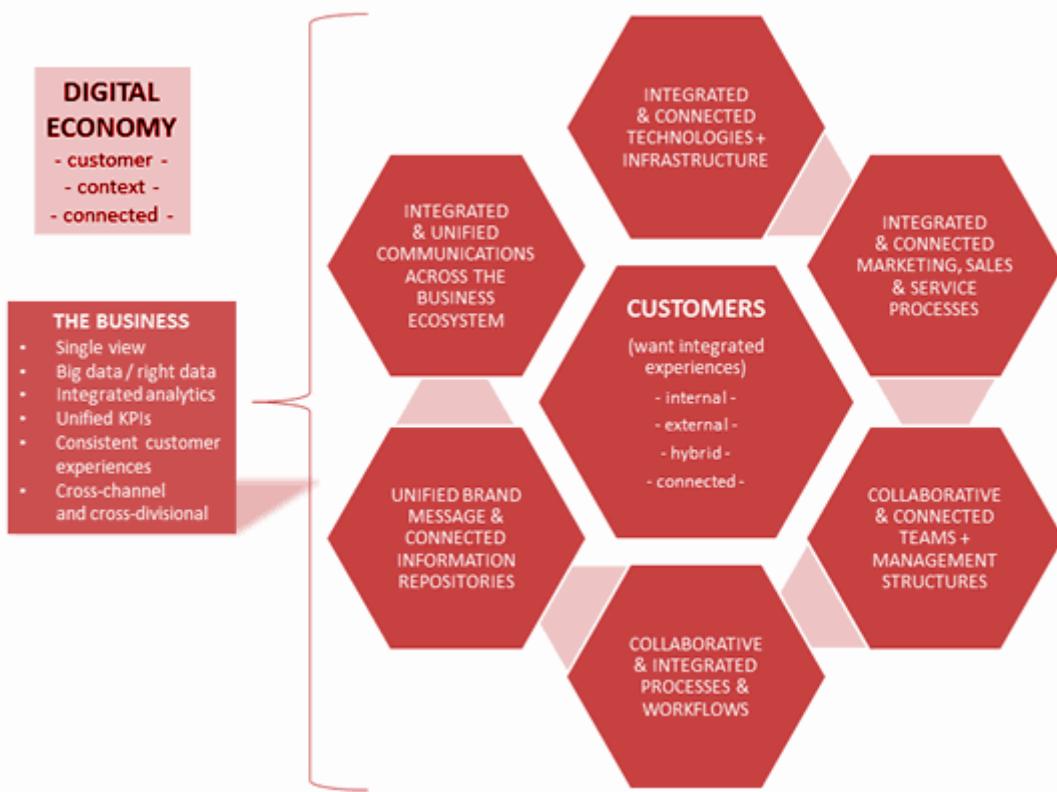
Evolution follows the accumulation of experience. All smart people learn from their mistakes; smarter people cut the curve by learning from others' missteps and victories. Change always carries a wealth of risks, still, sometimes risking nothing can risk everything.

80 percent of companies have realized that enslaving technology to do their bids has become crucial for their success, with the Fourth Industrial Revolution knocking on our doors. Again, only 29 per cent are able to state that they have already incorporated the managerial and technological merits of the new millennium.

The digital era has revolutionized the business world. Being competitive nowadays goes hand in hand with being innovative. Adapting to all those changes and especially doing so before the competition and in smarter ways can set a business apart from the packed crowd.

The obvious conclusion to be drawn, is that all of those movements are reinforced and heightened by Business Digitalization.



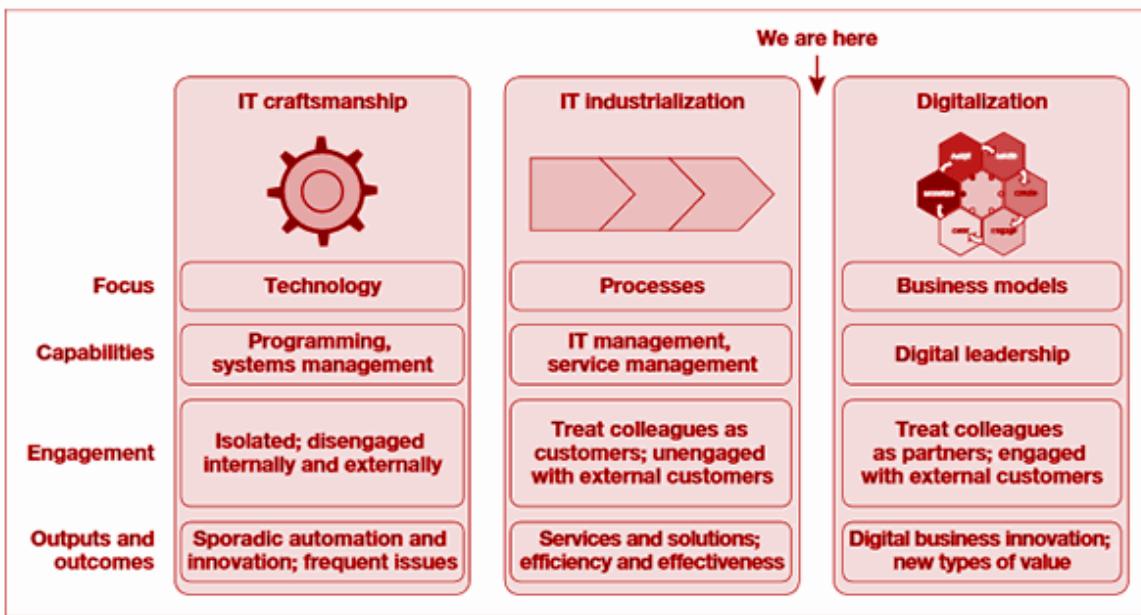


*Fig. 1: Business in Digital Economy*

## What is business digitalization?

Often used interchangeably with digitization and with complete digital transformation, digitalization is really something else.

Digitalization means the use of digital technologies and of data (digitized and natively digital) in order to create revenue, improve business, replace/transform business processes (not simply digitizing them) and create an environment for digital business, whereby digital information is at the core. And here we have three definitions, or better contexts in which the term is used.



*Fig. 2: Business History Timeline*

In business, digitalization most often refers to enabling, improving and/or transforming business operations and/or business functions and/or business models/processes and/or activities, by leveraging digital technologies and a broader use and context of digitized data, turned into actionable, knowledge, with a specific benefit in mind. It requires digitization of information but it means more and at the very center of it is data. While digitization is more about systems of record and, increasingly systems of engagement, digitalization is about systems of engagement and systems of insight, leveraging digitized data and processes.

A second aspect that is often mentioned is the digitalization of a specific ‘environment’ or area of business. Take the digital workplace. Often you strive towards a minimum of paper. But a digital workplace is about other things as well. It also means that your workforce works differently, using digital tools such as the mobile devices and technologies that make them mobile and/or using social collaboration and unified communication platforms, which are digital systems, enabling them to work in a more “digital way”. This, in turn, creates new opportunities to engage differently. And it requires more than just digitized data.

Digitalizing your business leads to digital business. The list of what you can digitalize (supply chains, leading to digital supply chains, etc.) is long. In general, digitalization is seen as the road of moving towards digital business and digital transformation, as

well as the creation of new – digital – revenue streams and offerings while doing so. And that requires change. This is why many people interchangeably use digitalization and digital transformation (so do we often).

A third meaning of digitalization goes beyond business and refers to the ongoing adoption of digital technologies across all possible societal and human activities. Think about, for instance, the increasingly digital customer, the rise of digital healthcare, the growing digitalization of government, of marketing, of customer service, etc. In other words: more digital (in various possible areas).

[ I-scoop.eu. (2018). *Digital business: transformation, disruption, optimization, integration and humanization.* [online] Available at: <https://www.i-scoop.eu/digital-business> ]

## Benefits of being a digital business



Img. 3: Top Perceived Benefits of Digitalization

As funny as it may sound, “Basic” is a term which describes the 20 percent of U.S. small businesses that aren’t using digital tools to their full advantage. The Deloitte Connected Small Businesses U.S. Research examined how digital tools help small businesses and, by implication, the U.S. economy. The study classified small

business owners into four digital engagement levels based on how they use online tools. Here's the breakdown:

- Basic (20 percent): Small businesses at this level have an undeveloped digital presence. They rely on traditional marketing methods, such as direct mail and print advertising. They have no website or social media presence. Essentially, the only digital tool they use is a business email address.
- Intermediate (30 percent): At this level, a small business uses digital tools such as a simple website (without e-commerce or mobile capabilities). It employs some basic online marketing tools, such as being listed in online directories or third-party marketplaces.
- High (30 percent): A high-level business has a more advanced website, such as one with mobile, online booking or e-commerce capabilities. It engages with multiple social media and online marketing channels. It also uses internal digital tools, such as videoconferencing or cloud software, to enhance the businesses productivity and effectiveness.
- Advanced (20 percent): This truly digital business uses all of the digital tools above, but at a higher level. In addition, they use more sophisticated digital tools, such as developing a mobile app or using data analytics to learn more about customer preferences or sales trends.
- The higher the digital engagement, the greater the benefits for a business, the survey found. This holds true no matter how long you have been in business, where your business is located, or what industry you're in. In fact, the gap between the accomplishments of basic and advanced (truly digital) small businesses is huge. Consider:

*Digital small businesses are job creators.* They are nearly three times as likely as basic businesses to have created jobs over the previous year. In addition, their employees tend to be more productive, thanks to the internal digital tools the company uses.

*Digital small businesses are reaching new markets.* With a wider variety of marketing outlets, they are able to reach a more diverse customer base, and as a result are three times as likely as basic businesses to have exported a product or service in the

last year. More than four in 10 (43 percent) of digital small businesses' customers are regional, national or international customers, compared to 28 percent for basic businesses.

*Digital small businesses are innovators.* High-level businesses are five times more likely, and advanced-level businesses almost 10 times more likely, to have introduced a new product or service in the past year as basic businesses.

*Digital small businesses are reaching more customers.* In the last year, they are almost three times as likely as basic businesses to have seen increased sales inquiries. In fact, digital small businesses experience more customer activity throughout the sales funnel, from interest to inquiries to purchase.

With all these factors in their favor, it's no wonder that digital small businesses are growing faster. Compared to basic small businesses, in the previous year digital businesses earned twice as much revenues per employee, and experienced revenue growth nearly four times as high. Expanding markets, innovative new products and services, and a growing customer base naturally lead to business growth.

To sum up, if a business hopes to grow — or even survive— it has to continuously improve the way it uses digital tools in its various procedures.

[Small Biz Daily. (2018). *The Benefits of Being a Digital Business* - Small Biz Daily. [online] Available at: <https://www.smallbizdaily.com/benefits-digital-business/> ].

### **The flipside of the coin**

If being a digital business is an idyllic situation or a one-way-street, why aren't all businesses already down on the road to digital transformation? Actually, they may be. Digitalization is a difficult and time-consuming procedure, which may also hide away many threats and obstacles and many businesses might even fail to transform. Moreover, maintaining a digital business could not be as easy as it seems, as threats may rise even after completing the transformation procedure and while regularly operating.

### **Digital threats to your business**

While the Internet, mobile computing and online advertising can help small fries compete with larger rivals, these digital tools also invite plenty of risk.

- Transaction Fraud
  - Pesky Intruders
  - Inside Job
  - Sloppy Software
  - Mobile Devices

Other issues, concerning more elaborate technical equipment and more advanced digital business models might include the following:

- Attacks on Internet of Things (IoT) devices
  - Data privacy
  - Point of sale (POS) attacks

[Forbes.com. (2018). [online] Available at: [https://www.forbes.com/2007/06/14/microsoft-apple-symantec-ent-tech-cx\\_df\\_0614riskdigital](https://www.forbes.com/2007/06/14/microsoft-apple-symantec-ent-tech-cx_df_0614riskdigital)]



*Img. 4: Digital Threats to your Business*

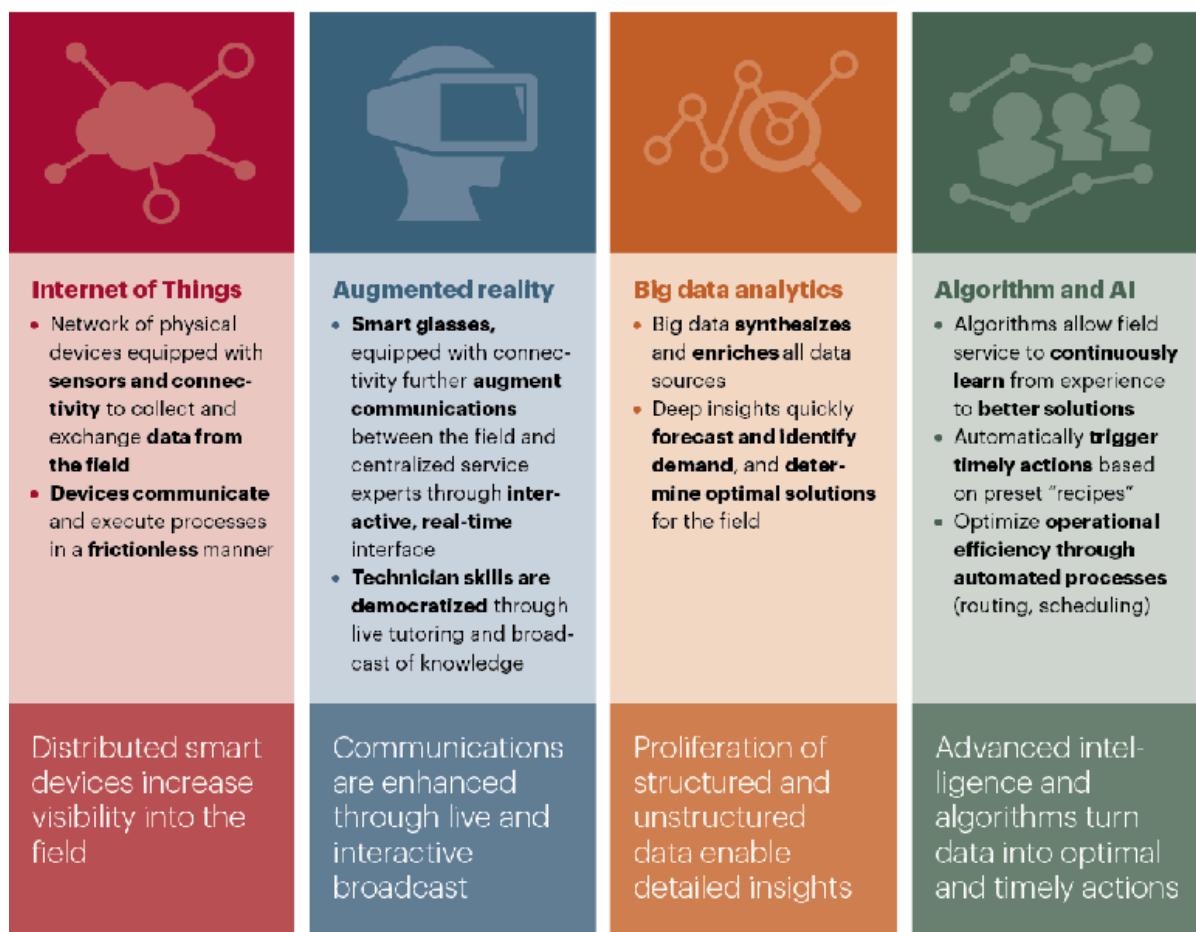
## Digital technologies towards business digitalization

Digital technologies are one of the most important sources of growth for national economies. They enable economies to create more jobs, improve people's lives and build better and greener societies. Citizens, enterprises, universities and governments become increasingly connected in the digital world. Digital is changing people's lives: the way they work, shop, socialize, communicate and educate. It also reshapes traditional industries and transforms the business environment, from fashion to automotive, from transport and logistics to energy distribution. New technological developments speed up and improve the way new innovative products and services are conceived, developed, produced and accessed. They are enabling businesses to faster develop and bring to market innovative products and services that it was impossible to think about before.

Digital technologies help to totally re-shape value chains, sharpen market intelligence, improve efficiency, reduce time-to-market and increase customer satisfaction. In addition, with the aid of technology, SMEs can now go global from day one, reaching overseas markets and talent pools instantly. Not surprisingly, organizations grow two to three times faster when they are empowered by digital technologies.

Modern collaboration technologies not only put a much larger and more diverse talent pool within reach of any entrepreneur starting or scaling a business; they allow talented individuals to work together in a seamless, global operation, despite being separated by time zones and geography.

Two still emerging and of great importance digital technologies for business are cloud computing and big data.



Img. 5: Digital Technologies is Opening New Opportunities

## B. Cloud-based solutions – Functionalities and Threats

### Cloud computing for business

Cloud computing provides a way for businesses to manage their computing resources online. The term has evolved over recent years, and can be used to describe the use of a third party for your storage and computing needs. The 'cloud' refers to the internet, and operating 'in the cloud' describes the way a business stores and accesses its data through an internet connection. Cloud computing allows businesses to access their information virtually, creating a flexible and global way of accessing your data any place, any time.



Img. 6: Cloud Computing for Business

## What is cloud computing?

The internet is changing the way we conduct business and interact as a society. Traditionally, hardware and software are fully contained on a user's computer. This means that you access your data and programs exclusively within your own computer.

Cloud computing allows you to access your data and programs outside of your own computing environment. Rather than storing your data and software on your personal computer or server, it is stored in 'the cloud'. This could include applications, databases, email and file services. A common analogy to describe cloud computing is renting versus buying. Essentially, you rent capacity (server space or access to software) from a cloud service provider, and connect over the internet. Instead of buying your own IT requirements, you are renting from a service provider, paying for only the resources you use.

Cloud computing has 4 models in terms of different access and security options. Before you move your data into the cloud, you will need to consider which model works best for your business and data needs.

### ***Private cloud***

A private cloud is where the services and infrastructure are maintained and managed by you or a third party. This option reduces the potential security and control risks, and will suit you if your data and applications are a core part of your business and you need a higher degree of security or have sensitive data requirements.

### ***Community cloud***

A community cloud exists where several organizations share access to a private cloud, with similar security considerations. For example, a series of franchises have their own public clouds, but they are hosted remotely in a private environment.

### ***Public cloud***

A public cloud is where the services are stored off-site and accessed over the internet. The storage is managed by an external organization such as Google or

Microsoft. This service offers the greatest level of flexibility and cost saving; however, it is more vulnerable than private clouds.

### ***Hybrid cloud***

A hybrid cloud model takes advantages of both public and private cloud services. By spreading your options across different cloud models, you gain the benefits of each model.

For example, you could use a public cloud for your emails to save on large storage costs, while keeping your highly sensitive data safe and secure behind your firewall in a private cloud.

## **How cloud computing works**

There are 3 main types of cloud computing service models available, commonly known as:

- Software as a Service (SaaS)
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)

Depending on your needs, your business could use one of these service models, or a mixture of the 3.

### ***Software as a Service (SaaS)***

SaaS is the most common form of cloud computing for small businesses. You can access internet-hosted software applications using a browser, rather than traditional applications stored on your own PC or server. The software application host is responsible for controlling and maintaining the application, including software updates and settings. You, as a user, have limited control over the application and configuration settings.

A typical example of a SaaS is a web-based mail service or customer relationship management system.

### ***Infrastructure as a Service (IaaS)***

IaaS typically means buying or renting your computer power and disk space from an external service provider. This option allows you access through a private network or over the internet. The service provider maintains the physical computer hardware including CPU processing, memory, data storage and network connectivity.

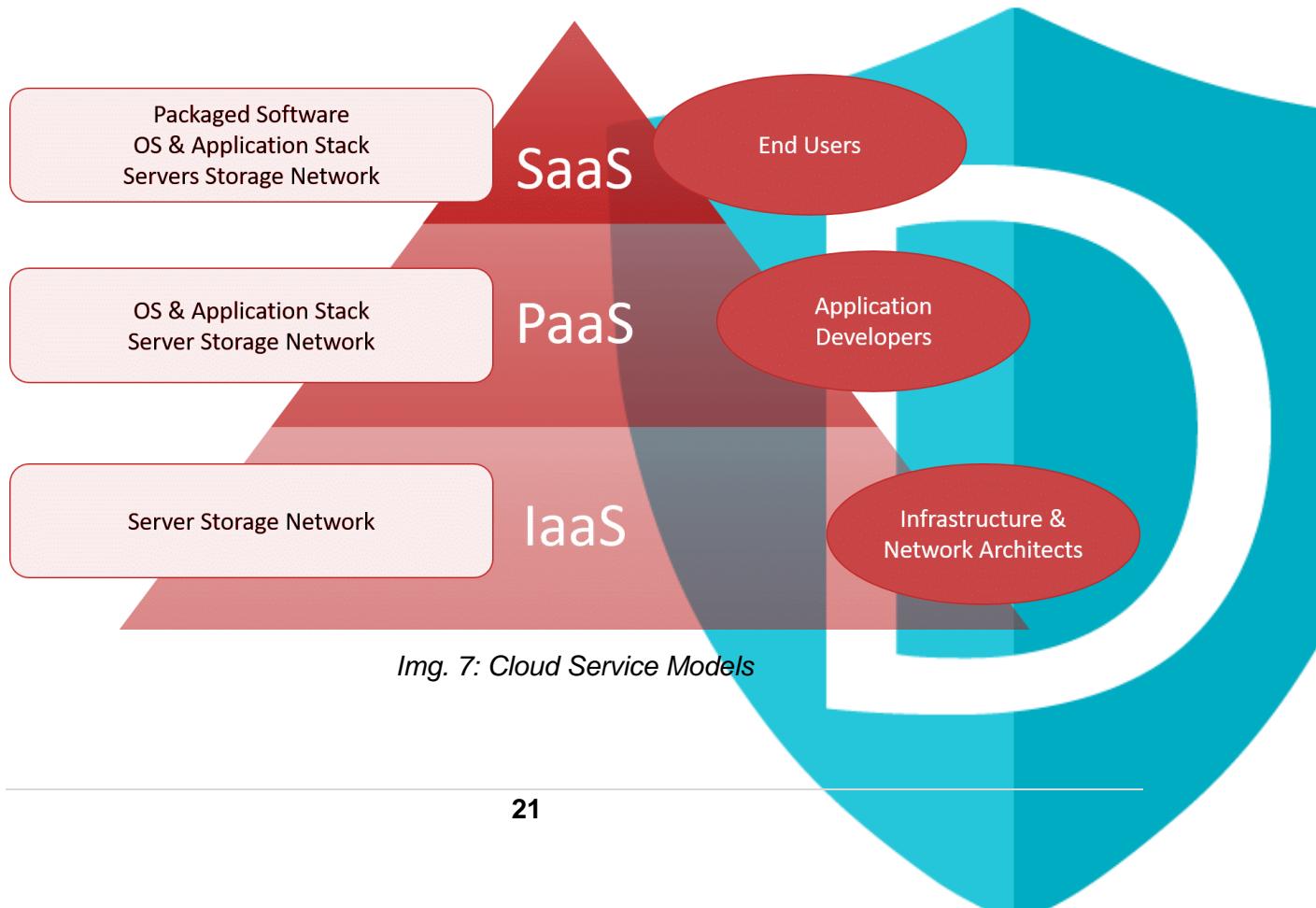
Examples of an IaaS include Amazon EC2, Rackspace and Windows Azure.

### ***Platform as a Service (PaaS)***

PaaS can be described as a crossover of both SaaS and IaaS. Essentially you rent the hardware, operating systems, storage and network capacity that IaaS provides, as well as the software servers and application environments. PaaS offers you more control over the technical aspects of your computing setup and the ability to customize to suit your needs.

[DreamHost. (2018). *What is Cloud Computing? Can It Help Your Business?* - DreamHost.blog. [online] Available at: <https://www.dreamhost.com/blog/cloud-computing-for-business>]

## **Cloud Service Models**



## How does cloud computing benefit a business?

Cloud computing offers your business many benefits. It allows you to set up what is essentially a virtual office to give you the flexibility of connecting to your business anywhere, any time. With the growing number of web-enabled devices used in today's business environment (e.g. smartphones, tablets), access to your data is even easier. Here's a closer look at 8 ways cloud computing can benefit your business:

### ***Simplicity***

Installing new software, keeping abreast of security issues, installing patches and upgrading to new versions of software is a full-time job. However, many small businesses can't afford an in-house IT specialist, so they outsource to IT consultants who are busy and not always able to stay on top of the business's IT needs. Other businesses rely on an "involuntary" IT person such as the company's office manager.

Either approach costs time, money and hassle and can even put your business at risk. If your business doesn't have an IT specialist on staff, using cloud-based software makes your life a lot easier. All of these updates are handled automatically off-site by the cloud services provider, which has a full staff of IT experts to provide up-to-the-minute technology. Even if your business does have IT specialists on staff, outsourcing to a cloud services provider enables your IT employees to spend less time on nuts-and-bolts maintenance issues and more time developing innovative ideas to grow your business.

### ***Security***

It seems that every day, we read about data breaches affecting huge corporations, such as Target, Home Depot, Sony etc. If such big companies aren't immune to malware, hackers and viruses, you can imagine how vulnerable your small business is. And while large companies can afford the fines and lawsuits associated with a data breach, such costs will put the typical entrepreneur out of business.

Don't assume you're safe because no one would bother to hack your business data. In reality, because small businesses are typically less protected from online threats, they are actually the preferred targets of online hackers. Reputable cloud services

providers can help by offering far better security than the average small business owner can provide. Storing your data in the cloud ensures it is protected by experts whose job is to stay up-to-date on the latest security threats.

### ***Continuity***

Natural disasters, theft or accidents can destroy your business's critical data if it's stored solely on hard drives or in-office servers. In recent years, extreme weather events such as floods, hurricanes and blizzards have put many small companies out of business—at least temporarily. Between 40 and 60 percent of small businesses affected by a disaster never reopen their doors, according to FEMA statistics.

Cloud storage and backup services can store continuously updated copies of your business data and applications online, so they're always safe from disaster and can be restored after an incident. Automated backup removes the risk of human error during the backup process, creating greater security. In addition, many cloud backup solutions offer the ability to save multiple versions of a document automatically, so you can easily go back to access earlier versions.

### ***Mobility***

Working remotely is a preferred perk for many employees these days. And, of course, busy small business owners often end up burning the midnight oil at home. When you use cloud services, you don't have to email yourself files for later, or remember to bring a thumb drive home. Instead, you and your team can access the latest versions of your documents and data from anywhere you have an Internet connection. Cloud services are a game-changer for salespeople and others who frequently travel on business to visit clients and prospects in person. Never again will you have to worry about leaving the latest version of a presentation, contract or proposal behind at your office.

### ***Efficiency***

Cloud-based software updates automatically, with no effort on your part. With no need for time-consuming maintenance on your end, your staff gains efficiency. Employees don't have to sit around waiting (and not working) while your IT specialist updates or fixes their computers. And since they always have the latest versions of

software, their computers are always running at peak performance. Fewer crashes and faster speeds mean your workers can get more done in less time.

### ***Connectivity***

Cloud services offer new ways to connect with remote or virtual employees, with customers and with prospects. For example, you can hold virtual conference calls or videoconferences online using cloud VoIP technology. Cloud-based collaboration tools allow teams to view, comment on and edit documents or presentations simultaneously in (almost) real-time. When there's no need to travel to a physical location to hold a meeting, your options for interacting with customers expand incrementally. That means more satisfied customers and stronger relationships.

### ***Affordability***

Cost savings is one of the cloud's biggest benefits for small businesses. Many cloud services providers offer free versions that are often suitable for a small company's needs. Instead of making a one-time payment for costly software, you pay for cloud services as you go, on a monthly or subscription basis. This pay-as-you-go model helps your cash flow, as costs are spread over time.

Cloud services cut your labour costs, too, since the cloud services provider handles tasks that would normally be done by an IT employee. Last, but not least, when using cloud services, you pay only for what you use. This ensures you aren't overspending on hardware you don't end up using, or buying software that your business quickly outgrows.

### ***Scalability***

Cloud services are a great way for small businesses to manage planned growth. As your company expands, you can easily switch to the next level of cloud services, add servers or add users almost instantly. There's no need to purchase costly new software or hardware, because you're just "renting" what you need from the cloud services provider. In addition to helping you deal with planned growth, cloud services also enable you to manage unexpected growth spurts. What if your product suddenly goes viral on social media and your business website is overloaded with visitors placing orders?

You can quickly solve the problem by scaling up to the next level of cloud-based services or adding new cloud-based tools. Cloud services can help with unexpected or seasonal slowdowns, too. If business declines, you eliminate a product or service, or you need to lay off staff, simply scale down the cloud services you are using. By providing simple, affordable scalability, cloud services enable small businesses to turn on a dime.

[ Business.qld.gov.au. (2018). *Cloud computing for business* | Business Queensland. [online] Available at: <https://www.business.qld.gov.au/running-business/it/cloud-computing> ]

### Join the crowd in the cloud

Clearly, cloud computing offers a host of advantages for small business owners. Perhaps the biggest is that it enables you to focus less on IT and more on your core business. With the flexibility and ease of cloud services, you can move quickly to take advantage of opportunity and grow your business to its full potential.

[ Business.qld.gov.au. (2018). *Cloud computing for business* | Business Queensland. [online] Available at: <https://www.business.qld.gov.au/running-business/it/cloud-computing> ]

### Cloud & data safety

Cloud safety is all about finding the right vendors and implementing technology that focuses on both identity verification and data encryption. Here are 10 security questions to ask cloud computing vendors before signing up for their services:

- Who can see my information?
- Is my data located at multiple data centers in different locations so it is protected from regional attacks?
- What redundancies do you have in place to protect my data?
- What specific measures do you take to encrypt my data?
- How do you manage encryption keys?
- What happens and how will you restore my data if there is a crash or cyberattack?

- What security certifications do you have?
- Are you compliant with the most current security protocols?
- What can go wrong during implementation?
- Are you a reseller? If so, who is responsible for service and support?



## C. Utilization of big data – Opportunities and Threats

### Big Data: What it is and why it matters



Img. 8: Big Data Application

Big data is a term that describes the large volume of data – both structured and unstructured – that inundates a business on a day-to-day basis. But it's not the amount of data that's important. It is what organizations do with the data that matters. Big data can be analyzed for insights that lead to better decisions and strategic business moves.

In defining big data, it's also important to understand the mix of unstructured and multi-structured data that comprises the volume of information.

**Unstructured data** comes from information that is not organized or easily interpreted by traditional databases or data models, and typically, it's text-heavy. Metadata, Twitter tweets, and other social media posts are good examples of unstructured data.

**Multi-structured data** refers to a variety of data formats and types and can be derived from interactions between people and machines, such as web applications or social networks. A great example is web log data, which includes a combination of text and visual images along with structured data like form or transactional information. As digital disruption transforms communication and interaction channels—and as marketers enhance the customer experience across devices, web properties, face-to-face interactions and social platforms—multi-structured data will continue to evolve.

[Forbes.com. (2018). [online] Available at: <https://www.forbes.com/sites/lisaarthur/2013/08/15/what-is-big-data>]

## Why Is Big Data Important?

The importance of big data doesn't revolve around how much data you have, but what you do with it. You can take data from any source and analyze it to find answers that enable:

1. cost reductions
2. time reductions
3. new product development and optimized offerings, and
4. smart decision making.

When you combine big data with high-powered analytics, you can accomplish business-related tasks such as:

- Determining root causes of failures, issues and defects in near-real time.
- Generating coupons at the point of sale based on the customer's buying habits.
- Recalculating entire risk portfolios in minutes.
- Detecting fraudulent behavior before it affects your organization.

## How can businesses benefit from big data?



*Fig. 9: Benefits for Businesses from Using Big Data*

- Using big data cuts your costs

A recent Tech Cocktail article looks at how Twiddy & Company Realtors cut their costs by 15%. The company compared maintenance charges for contractors against the average of its other vendors. Through this process, the company identified and eliminated invoice-processing errors and automated service schedules.

- Using big data increases your efficiency

Using digital technology tools boosts your business's efficiency. From using tools such as Google Maps, Google Earth, and social media, you can do many tasks right

at your desk without having travel expenses. These tools save a great amount of time, too.

- Using big data improves your pricing

Use a business intelligence tool to evaluate your finances, which can give you a clearer picture of where your business stands.

- You can compete with big businesses

Using the same tools that big businesses do allows you to be on the same playing field. Your business becomes more sophisticated by taking advantage of tools that are available for your use.

- Allows you to focus on local preferences

Small businesses should focus on the local environment they cater to. Big Data allows you to zoom in on your local client's likes/dislikes and preferences even more. When your business gets to know your customers' preferences combined with a personal touch, you'll have an advantage over your competition

- Using big data helps you increase sales and loyalty

The digital footprints that we leave behind reveal a great deal of insight into our shopping preferences, beliefs, etc. This data allows businesses to tailor their products and services to exactly what the customer wants. A digital footprint is left behind when your customers are browsing online and posting to social media channels.

- Using big data ensures you hire the right employees

Recruiting companies can scan candidate's resumes and LinkedIn profiles for keywords that would match the job description. The hiring process is no longer based on what the candidate looks like on paper and how they are perceived in person.

[King, A. (2018). *7 Benefits to Using Big Data for Small Businesses* - IndustriusCFO. [online] IndustriusCFO. Available at: <http://www.industriuscfo.com/7-benefits-using-big-data/>]

## D. Improving Digital Skills of Employees

### **Business Digitalization Barriers and Digital Skills**

Digital transformation is changing every aspect of the business landscape, provided that leaders are ready to embrace it. What's the state of digital disruption and what should businesses expect?

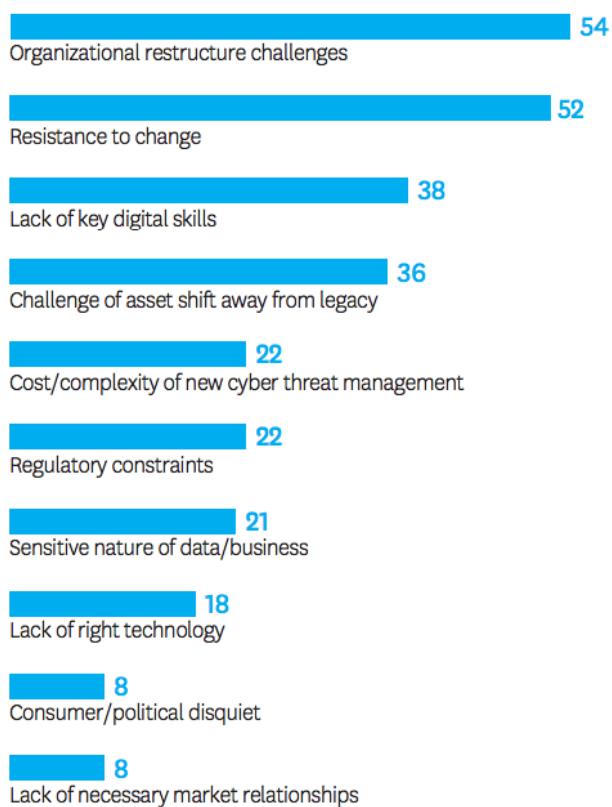
We are already experiencing a period of digital transformation, and the businesses that already acknowledge it enjoy its benefits. But what can we expect from the next few years, and how can businesses keep pace with the changes affecting their industry?

Harvard Business Review Analytics Services and Microsoft published the report, "Competing in 2020: winners and losers in the digital economy" to give an overview of the state of digital disruption and how business leaders are reacting to it. One of the most noteworthy points to consider in this particular survey was the connection attempted among business digitalization barriers and digital skills.

Digital transformation does not come without challenges, and there are many barriers to its integration in a business. Respondents of the survey were asked to identify the most significant barriers towards adapting to digital transformation within the coming years; 54% of them named their organization's structure as the biggest challenge.

**BARRIERS TO FUTURE TRANSFORMATION**

Percentage of respondents citing obstacles to digital transformation

**SOURCE** HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, DECEMBER 2016*Fig. 10: Barriers to Future Transformation*

A very similar percentage (52%) named resistance to change as a key barrier to digital transformation in their business, while other responses included a lack of digital skills, resources and budget. The resistance to change is probably the most interesting challenge identified, as it indicates that some organizations are not receptive to new trends. This may require further collaboration and training to help them understand the benefits of digital disruption to their services.

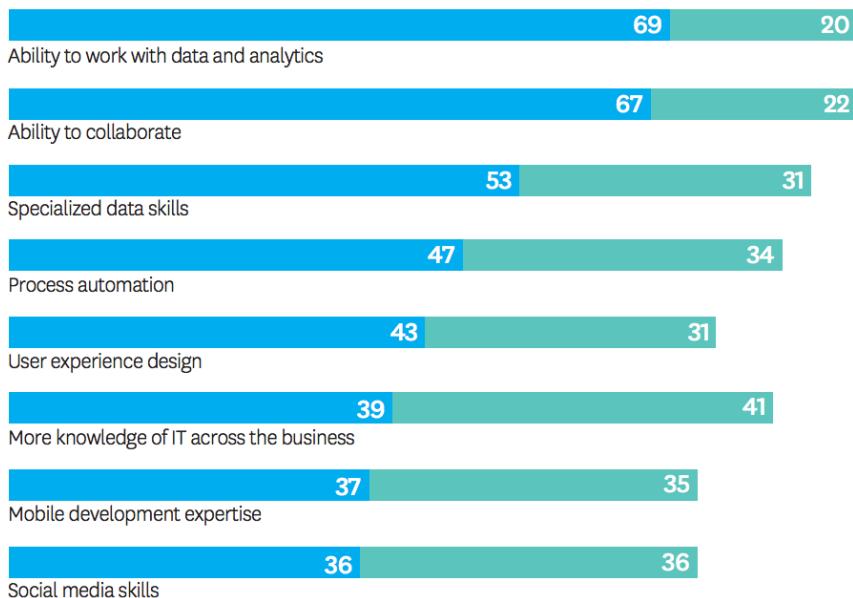
Moreover, the lack of resources, budget and skills cannot be overlooked, with the latter creating the need for everyone to develop the right traits that make a digital leader. According to respondents, the most important skill that digital leaders need to have for 2020 is the ability to work with data and analytics, with focusing on specialized data skills ranked third in the list. The ability to collaborate was the second most popular skill, with respondents clearly recognizing the need for more

people in their organization to develop the right skills to embrace digital transformation.

### MOST IMPORTANT SKILLS FOR 2020

Percentage of respondents who cite how important each will be for their organization's success in 2020

● VERY IMPORTANT ● SOMEWHAT IMPORTANT



SOURCE HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, DECEMBER 2016

Img. 11: Most Important Skills for 2020

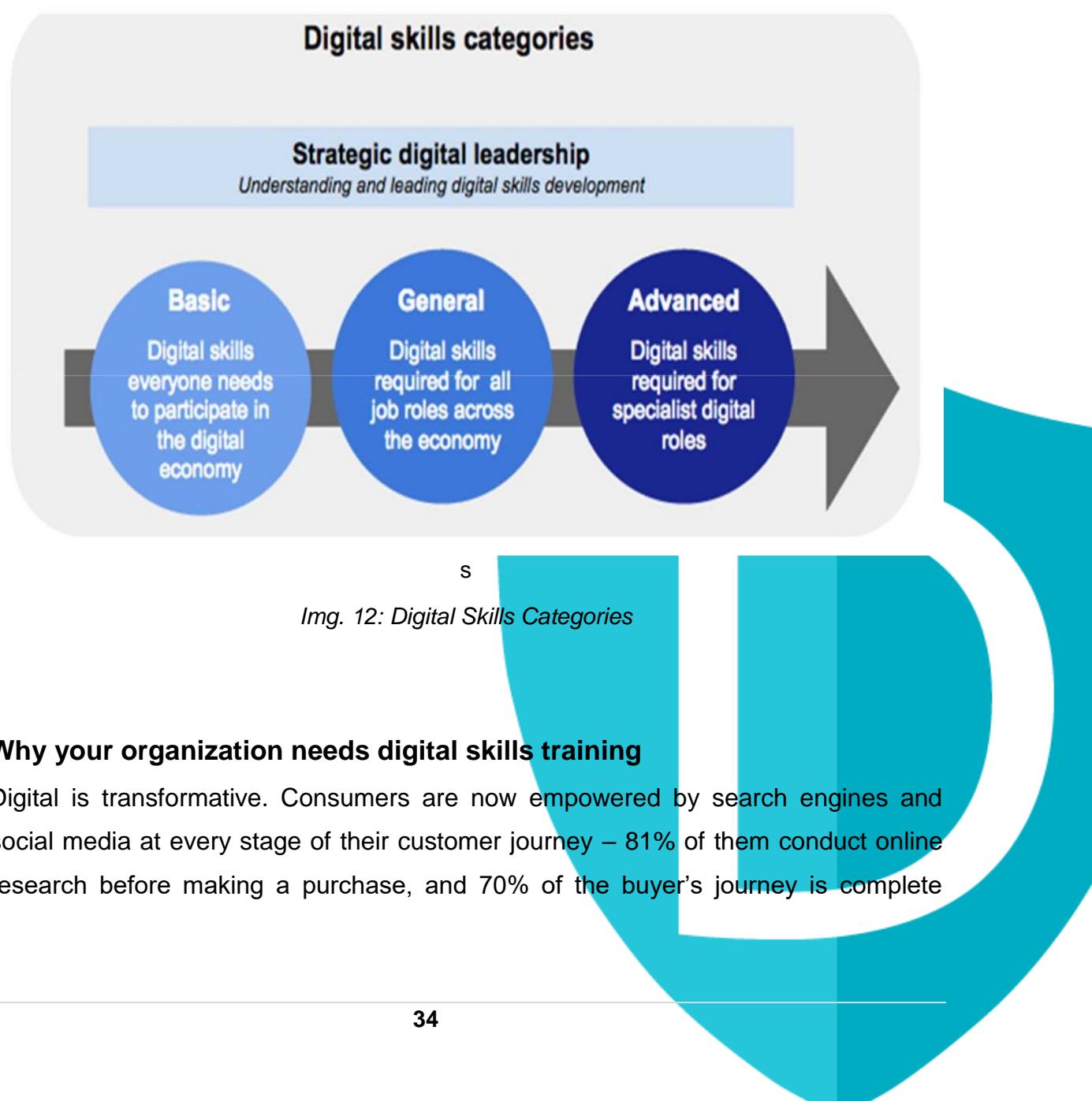
[The rising opportunity of digital transformation: What businesses need to know - ClickZ. [online]. Available at: <https://www.clickz.com/the-rising-opportunity-of-digital-transformation-what-businesses-need-to-know/110987/>]

### What are Digital Skills?

Digital skills draw their roots from stratified and complex convergence of several key skills concepts, namely IT literacy, ICT literacy, digital literacy, digital competence, ICT fluency, computer literacy, ICT skills, e-Skills, technological literacy, media literacy, information literacy, e-literacy, generic skills, 21st century skills, multi-literacies, and new literacies. Glister is credited with the widespread of use of the

term digital literacy, which he described as the: ability to understand and use information in multiple formats from a wide range of sources when it is presented via computers.

Digital skills involve the knowledge and ability to determine information needs from digital technology sources, and to appropriately use digital tools and facilities to input, access, organize, integrate and assess digital resources as well as to construct new knowledge, create media expressions and communicate with others. Digital skills include both technical skills associated with understanding and using digital systems, tools, and applications, as well as information processing skills, which are the cognitive underpinnings of digital proficiency.



before they reach out to a sales rep. Digital has enabled consumers to self-educate, and be much more scrupulous when making their definitive purchase decision.

This creates an obligation for organizations to acknowledge and adapt to this digital growth if they want to achieve lasting customer success and be as profitable as possible. 76% of marketers think that marketing has changed more in the past two years than the past fifty, which means that continual upskilling is essential.

Organizations who make the decision to engage customers and prospects with a well-considered digital marketing strategy will find it easier to build brand awareness, generate cost savings, and ultimately drive revenue. This is why skilled digital professionals are an indispensable asset.

Yet despite the unquestionable benefits that digital brings, a high volume of organizations remains resistant to the use of digital tools and technologies. Whether it's a lack of available budget and resources, a fear of loss of control or a general scepticism that digital can provide a significant return on investment, these barriers to digital adoption must be overcome to guarantee ongoing organizational success.

The answer is simple. A short term investment in digital skills training will result in long term reward - empowering an organization and its employees, maintaining their competitive advantage and ensuring they don't get left behind.

If you're still in any doubt as to how your organization could benefit from a strategic, sustainable digital education plan, take a look at some key advantages below:

### *1. Digital skills can motivate employees*

Currently, there is an unprecedented global digital skills shortage affecting all industries. As a result, the recruitment of competent candidates presents a problem to organizations of every size.

As they are in competition with each other to hire the few digitally engaged professionals that exist, smaller businesses suffer, failing to match the increasingly lucrative salaries and benefit packages easily offered by their corporate competitors.

Yet despite this urgent demand, digital skill levels worldwide are staggeringly low. In a 2016 Digital Skills Report, marketers across Ireland, the UK and the USA, when tested on their digital competence, scored just 38% on average. This is coupled with

a widespread acknowledgment that they will need to improve their digital marketing skills to remain competent in their roles (86% Ireland, 69% UK and USA).

More and more, companies are looking to hire skilled professionals internationally as a solution to this scarcity of talent. However, the easier, and ultimately more cost-effective option is to cultivate an indigenous talent pool.

According to Adobe, organizations with a plan for their digital maturity aim to train and develop the skills of their existing workforce. They recognize that training, and the opportunity for professional and personal development is often a main priority for employees. Without it, they can feel unstimulated and disillusioned.

If organizations empower their employees with a digital education, not only will they benefit from their new digital capabilities and incentivized attitude, they can leverage the training as a powerful retention tool as well.

## *2. Digital skills can help to drive more revenue*

Digital tools and technologies have already had a profound impact on the global economy. In 2016, global online advertising revenue surpassed TV advertising for the first time, and total digital advertising revenue is forecasted to reach over 260 billion US dollars by 2020.

Digital ad spent and marketing budgets are systematically expanding as a growing number of organizations have begun to acknowledge the business benefits that digital can bring. According to a report from Capgemini, companies with stronger digital intensity derive more revenue from their physical assets and are between 9 to 26% more profitable.

There have been too many technological advancements for organizations to thrive on traditional marketing and selling approaches alone. Only 28% of prospects that are cold call actually engage in conversations, and only 1% of those cold calls will ultimately convert into appointments. As consumers become more empowered by digital, they rely less on the expertise of sales reps and more on their own ability to research. In response to this shift in power, organizations need to revitalize their sales and marketing functions and utilize the same channels and platforms their customers do in order to reach them effectively.

Digital skills can enable your organization to better nurture its customer relationships, establish itself as an industry thought-leader and convert more buyers throughout the customer journey. Digital skills training will release this potential.

### *3. Digital skills can generate significant cost savings*

We've all heard the phrase "spend money to make money". But what about spending money to save money too? With a complete digital skillset, your organization can achieve both.

The American Society for Training and Development (ASTD) collected training information from over 2500 firms and found that organizations that offer comprehensive training have 218% higher income per employee than those with less comprehensive training. This means the simple act of motivating employees through skills training can save a substantial amount of money for an organization. Similarly, according to the American Management Association, the cost of hiring and training a new employee is between 25 to 200% of annual compensation, so skills training can cut costs again by alleviating unnecessary employee turnover. In addition to this, other financial benefits can include labour savings, reduction in lost workdays and productivity increases.

Digital marketing's main principles are based on efficiency and cost-effectiveness:

- Precise ad targeting options can result in a lower Cost-Per-Lead
- Easy and immediate online interactions with a segmented target audience can generate more conversions for less cost
- An abundance of data from analytics tools provide invaluable insight that can help to refine a digital strategy and avoid unnecessary spending.

According to Gartner, 40% of organizations claimed they received considerable cost savings from using digital marketing methods to promote their products and services. These savings can then be taken and reinvested into more digital marketing techniques and tactics to reiterate revenue success at a lower overall expenditure.

### *4. Digital skills can help your organization to develop a competitive edge*

A strong digital skillset is no longer a luxury for organizations – it's a fundamental element of any competitive business model. Yet despite this, our latest skills report

found that organizations remain largely disengaged with digital. Only 31% of US organizations, 25% UK and 40% in Ireland are felt to be digitally engaged, and the general consensus among employees is that the pace of technological and digital change is too slow.

According to McKinley, 90% of all marketing roles now require digital skills. This is because digital specialisms are infinitely more targeted, efficient and measurable in comparison to traditional techniques. Digital is a data-driven enabler for success. It can streamline processes and the accompanying effort required, whilst expanding capabilities. Being able to gain precise insights and translate those insights into actions means that, if leveraged successfully, digital tools and channels can help organizations to develop, and maintain an impactful competitive advantage.

Social media can provide a platform for meticulous online customer service that will improve retention rates. Mobile marketing can help an organization to develop a ubiquitous brand presence. Email marketing can nurture valuable relationships through useful content at every stage of the customer journey. And every campaign you construct can be measured and optimized using analytics tools.

Some of the main barriers to digital adoption is a lack of expertise in-house, as well as a lack of organizational commitment to the area. In order to realize the potential that digital holds for your organization, it's essential to have the requisite skills training to be able to understand its significant benefits and take action.

[Digital Marketing Institute. (2018). *Why your organization needs digital skills training*. [online] Available at: <https://digitalmarketinginstitute.com/blog/why-your-organization-needs-digital-skills-training>]

## E. Business Digitalization Checklist

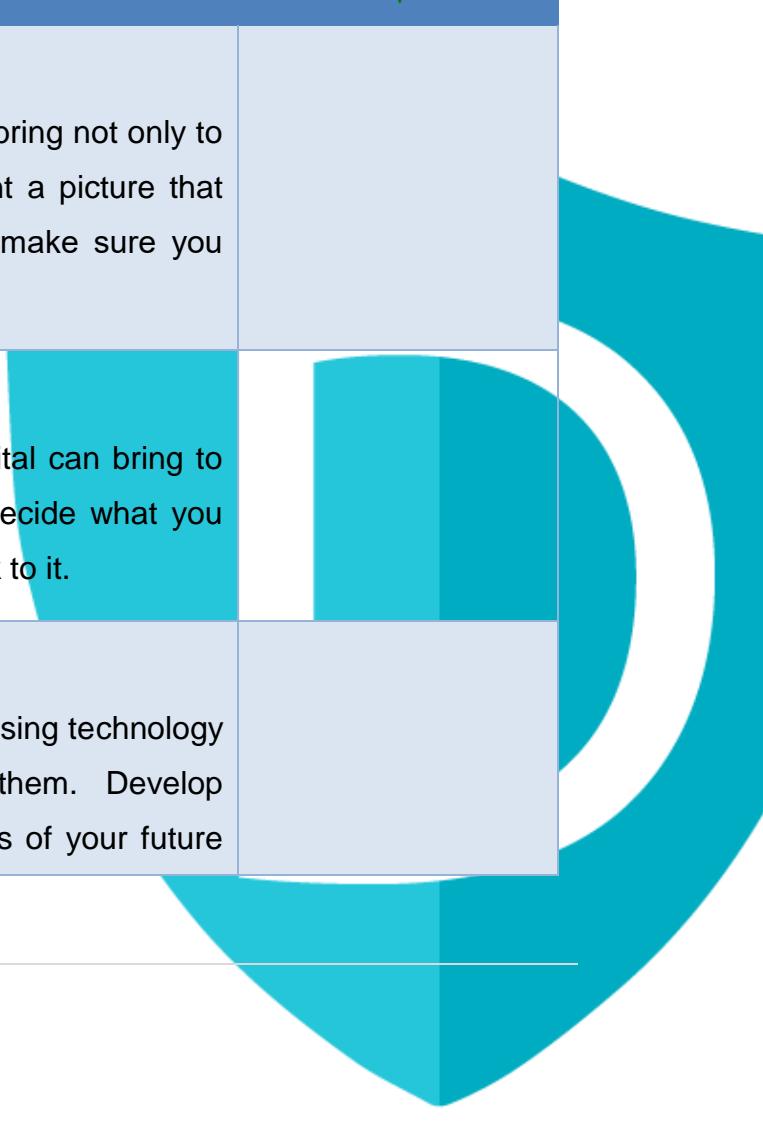
### Are you ready for the digital era?

Many small business owners believe that they are already using digital technology effectively, because they have a website and Facebook page. But there are many more ways to use digital technology to improve your business outcomes.

Conducting a digital audit will help you work out whether your business is a digital novice, digitally active or digitally advanced.

### Digitalization: The 10-step checklist to get started with

The path towards digitalization may be long. To make sure you won't get lost, you should start at least with the following:



<b>Get the team on board</b>  Outline the major benefits that digitizing will bring not only to your company – but to all employees. Paint a picture that gets everyone excited. If you're the CEO, make sure you take a visible role in promoting the change.	
<b>Commit to a vision</b>  Imagine the tangible benefits that going digital can bring to your business, company and community. Decide what you want to achieve from going digital – and stick to it.	
<b>Understand your future customers</b>  Keep an eye on your millennial customers. Using technology in everyday life is second nature to them. Develop technology solutions now to meet the needs of your future	

customers – and keep pace with your future competition.	
<b>Map out the digital journey</b>  Take a look at how your current and target customers use digital platforms. This will help you identify the right digital solutions needed to reach them.	
<b>Set up a digital working group</b>  Involve all of your employees by setting up a working group of digital champions. This will help secure ‘buy-in’ across business areas. The working group can collaborate on the delivery timeline, maintain project schedules and keep their teams updated on progress.	
<b>Invest in the right tools</b>  Research the appropriate, industry-specific software and IT tools for your digital business. From accounting, inventory management, point-of-sale, payroll and more – there are literally hundreds of applications that can help your business. These feature data security, mobile access, real-time reporting and integration to help make for a smooth and seamless transition.	
<b>Embrace a SaaS platform</b>  Turn to the right SaaS (Software as a Solution) platform to better use and manage your important business data. SaaS tools that talk to each other on one platform can eliminate manual data entry – and that means more time for you to run your business. SaaS providers also have the highest levels of security, so you can rest assured that all of your information is in safe hands.	
<b>Cut your losses</b>	

Demonstrate your bold leadership by making tough decisions. Know what something can and can't do and, more importantly, its place within your digital transformation strategy. If this requires you to write-off non-performing investments in old systems and software - take the plunge.	
<b>Measure results</b>  Keep track of how your digital initiatives impact your numbers. Compare to your original goals and reflect on whether your approach is consistently helping you achieve the best results.	
<b>Share your new knowledge</b>  Train your team to ensure that your employees have the skills, knowledge and experience to get the most out of your digital strategy.	



## F. Terminology glossary

**Big data** - Big data is data sets that are so voluminous and complex that traditional data-processing application software are inadequate to deal with them. Big data challenges include capturing data, data storage, data analysis, search, sharing, transfer, visualization, querying, updating, information privacy and data source.

**Cloud computing** - Cloud computing is an information technology (IT) paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility.

**Digital Business** - Digital business is the creation of new business designs by blurring the digital and physical worlds.

**Digital Disruption** - Digital disruption is an effect that changes the fundamental expectations and behaviors in a culture, market, industry or process that is caused by, or expressed through, digital capabilities, channels or assets.

**Digital Skills** - Digital skills are any skills related to being digitally literate.

**Digitalization** - Digitalization is the use of digital technologies to change a business model and provide new revenue and value-producing opportunities; it is the process of moving to a digital business.

**Machine Learning** - machine learning algorithms are composed of many technologies (deep learning, neural networks and natural-language processing), used in unsupervised and supervised learning, that operate guided by lessons from existing information.

**Platform (Digital Business)** - a platform is a product that serves or enables other products or services. Platforms (in the context of digital business) exist at many levels. They range from high-level platforms that enable a platform business model to low-level platforms that provide a collection of business and/or technology capabilities that other products or services consume to deliver their own business capabilities. Platforms that enable a platform business model have associated business ecosystems.

## G. Conclusions and Further Reading

Undoubtedly, digital transformation will be the game changer for a range of industries. It is the next phase of industrial revolution. Business digitalization is not actually digital transformation of a business, yet it is a key step towards this direction.

Despite the importance business digitalization seems to have, it is not an easy path to go through. Over half of European C-suite executives say digital innovation has not delivered high business impact at their organization. Frequently corporations believe that digital is merely a new channel, and are unclear what they can expect.

It is definitely a challenging task to stay on top of the multitude of digital technologies such as AI, biometrics, quantum computing and robotics. However, when companies put the customer right at the centre of their digital innovation, and use digital technologies to create wow-experiences for them, we see over and over again that high impact is the result. Businesses frequently set up “digital” as a project, but this setup cannot deliver high business impact.

Digital technologies fundamentally change how companies go to market and how they organize themselves internally. For digital technologies to deliver high impact, the whole organization needs to be taken along, and needs to buy into this new way of thinking.

Companies that believe integrating new technologies into established (legacy) infrastructure is their key challenge in digital innovation have started from the wrong angle. Digital technologies are not here to fix something that does not work. Digital technologies allow companies to fundamentally rethink what they go to market with, how they go to market and who to go with.

Keeping the whole team, the people behind the business aligned towards this change is of critical importance, as well. Employees need to possess those certain skills that will help them embrace the change and perform efficiently in the new digital environment.

Seems that humans are the most significant factor for new technologies to successfully merge to the business environment and become the tool for thriving for success.

**Further reading:**

To effect digital transformation, you need to be fully steeped in the workings of machine learning and AI. You should also be aware of the Blockchain revolution: and how the technology behind Bitcoin is changing money and business, as sooner or later, every organization will need to understand and use blockchain in some form. The ability to pick the right team, bring them together with a shared vision, and motivate them to achieve more than they thought they could, is also a skill you should further elaborate. Big Data - you've watched Big Data transform the world of IT and the world of business. But in many ways, this trend is just getting started. Many leaders still don't understand or embrace the power of data to drive decisions, large and small. Understand the capabilities Big Data open, as well as the threats behind them. You may also study the way start-ups work and how they use continuous innovation to create radically successful business. There's a reason that start-ups so frequently disrupt larger, more established organizations -and this is it. Applying the principles of lean and agile to your own organization and technology will help you adapt to a rapidly changing marketplace and make you less vulnerable. It might even help you create some disruption of your own.



## H. References

- 1.i-scoop: Digitization, digitalization and digital transformation: the differences  
[\(https://www.i-scoop.eu/digitization-digitalization-digital-transformation-disruption\)](https://www.i-scoop.eu/digitization-digitalization-digital-transformation-disruption)
- 2.Gartner Executive Programs: Taming the Digital Dragon: The 2014 CIO Agenda
- 3.i-scoop: Digital business: transformation, disruption, optimization, integration and humanization  
[\(https://www.i-scoop.eu/digital-business\)](https://www.i-scoop.eu/digital-business)
- 4.tieto: How Digitalization is Changing the Face of Business  
[\(https://perspectives.tieto.com/blog/2015/07/how-digitalization-is-changing-the-face-of-business\)](https://perspectives.tieto.com/blog/2015/07/how-digitalization-is-changing-the-face-of-business)
5. Forbes: Digital Business is Everyone's Business  
[\(https://www.forbes.com/sites/gartnergroup/2014/05/07/digital-business-is-everyones-business/#7f60b8b67f82\)](https://www.forbes.com/sites/gartnergroup/2014/05/07/digital-business-is-everyones-business/#7f60b8b67f82)
6. cio: Digital transformation: Why it's important to your organization  
[\(https://www.cio.com/article/3063620/it-strategy/digital-transformation-why-its-important-to-your-organization.html\)](https://www.cio.com/article/3063620/it-strategy/digital-transformation-why-its-important-to-your-organization.html)
- 7.insightsuccess: Role of Digitization in Today's Business World  
[\(https://www.insightssuccess.com/role-of-digitization-in-todays-business-world\)](https://www.insightssuccess.com/role-of-digitization-in-todays-business-world)
- 8.Forbes: Digital Transformation And Innovation In Today's Business World  
[\(https://www.forbes.com/sites/brianrashid/2017/06/13/digital-transformation-and-innovation-in-todays-business-world/#341a36e74905\)](https://www.forbes.com/sites/brianrashid/2017/06/13/digital-transformation-and-innovation-in-todays-business-world/#341a36e74905)
- 9.McKinsey & Company: Raising your Digital Quotient  
[\(https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/raising-your-digital-quotient\)](https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/raising-your-digital-quotient)
10. Deloitte: Doing business in the digital age: the impact of new ICT developments in the global business landscape (April 2013)
- 11.Gartner: The New Risks of Digital Business

(<https://www.gartner.com/smarterwithgartner/the-new-risks-of-digital-business>)

12.i-scoop: Cybersecurity: security risks and solutions in the digital transformation age

(<https://www.i-scoop.eu/cyber-security-cyber-risks-dx>)

13.wired: 5 cloud business benefits

(<https://www.wired.com/insights/2012/10/5-cloud-business-benefits>)

14. dreamhost: What is Cloud Computing and How Can It Help Your Small Business?

(<https://www.dreamhost.com/blog/cloud-computing-for-business>)

15.McKinsey & Company: How companies are using big data and analytics

(<https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/how-companies-are-using-big-data-and-analytics>)

16. Business News Daily: 8 Big Data Solutions for Small Businesses

(<https://www.businessnewsdaily.com/6358-big-data-solutions.html>)

17.sas: How Midsized Businesses Can Take Advantage of Big Data (white paper)

18.Bernard Marr & Co: How Is Big Data Used In Practice? 10 Use Cases Everyone

#### Must Read

(<https://www.bernardmarr.com/default.asp?contentID=1076>)

19. Digital Skills Academy: The Top 10 Digital Skills Tech Companies are Looking for Today

(<https://digitalskillssacademy.com/blog/the-top-10-digital-skills-tech-companies-are-looking-for-today>)

20.Skillsoft: What are digital skills? A comprehensive definition for modern organisations (white paper)

21.Digital Marketing Institute: Why your organization needs digital skills training

(<https://digitalmarketinginstitute.com/blog/why-your-organization-needs-digital-skills-training>)

22.Department for Culture, Media and Sports, France: Digital Skills for the Digital Economy

23. Smallbizdaily.com: The Benefits of Being a Digital Business

(<https://www.smallbizdaily.com/benefits-digital-business/>)

24. Forrester: Why Do Digital Business Transformations Fail?

(<https://go.forrester.com/blogs/15-04-01-why-do-digital-business-transformations-fail/>)

25. Business Queensland: Cloud computing for business

(<https://www.business.qld.gov.au/running-business/it/cloud-computing>)

26. Business News Daily: Cloud Computing: A Small Business Guide

(<https://www.businessnewsdaily.com/4427-cloud-computing-small-business.html>)



## **SECTION II**

**DIGITAL SECURITY FOR  
YOUNG SOCIAL  
INNOVATORS**

## List of abbreviations

Abbreviation	Definition
SBI	Social Business Initiative
SME	Small and medium-sized enterprises
IoT	Internet of things
SEO	Search Engine Optimization
IT	Information Technology



## A. Introduction

The following chapters will give social enterprises and social innovators an insight on the concept of social entrepreneurship in the digital era and how the working environment has modified from the in-office traditional environment to the digital environment in the sphere of IoT. The chapter will also highlight the opportunities and threats of the social business in the online environment and suggest how to properly implement the business to avoid any harmful effects of doing business in the online sphere. The chapter will provide social innovators and entrepreneurs with tips and useful checklist for implementing digital security in their social businesses.

*“One enterprise can be social only when the social goals are the main mission of its activity. [11] “*



## B. Social Entrepreneurship in the Digital Era

It is evident that social enterprises today have a strong positive impact on the society and even more, they appear to be a buffer for negative consequences produced by the economic crisis.

*“Social entrepreneurship was one of the main topics discussed at the World Economic Forum, held in Davos in January 2017, as a new way or a tool for overcoming certain social ills that plague contemporary societies [1].”*

Moreover, the business environment has shifted from the in-office, more traditional business environments to the digital business environment, which also ensures a different business approach for the companies, one that is far more adaptable to change than before. The digital environment, innovation and emerging technologies are opportunities for businesses to take into account in their daily operations, however, they also pose threats if not implemented accordingly. If these tools are to have the proper impact on one's business, they should be integrated accordingly and should be a focus for the business to have proper digital security risk management and privacy strategy [1].

However, businesses often do not sufficiently understand how digital security and privacy issues can create economic risks and have limited capacity to respond and manage them. While different types of SMEs face different challenges, all would benefit from integrating digital security and privacy risk management into their business decision-making.

In the current digital age, services in various business areas need to run uninterrupted, 24 hours a day, 365 days a year. While progress has been made in providing services more efficiently through technologies such as IoT, the methods of cyber-attacks have become increasingly diverse and sophisticated - even verging on cyberterrorism. That is why security within the system is essential [2].

*“The Internet, social networking websites and social media have been pivotal resources for the success and collaboration of many social entrepreneurs. In the 2000s, the Internet has become especially useful in disseminating information to a wide range of like-minded supporters in short amounts of*

*time, even if these individuals are geographically dispersed. In addition, the Internet allows for the pooling of design resources using open source principles” [3].*

As already established, any kind of enterprise but especially social enterprises have to adapt to the speed, environment and the demands of the digital are and have to adapt their products, services, business, partnerships, business dealing to the digital environment. But when thinking of adapting to the digital world, the businesses more often neglect the revers angle what opportunities lie if one digitalises their business. What can the digital environment do for the business?

Such examples are the use of wiki models or crowdsourcing approaches, for example, a social enterprise can get hundreds of people from across a country (or from multiple countries) to collaborate on joint online projects (e.g., developing a business plan or a marketing strategy for a social entrepreneurship venture). Here is a list of crowdfunding sites that seek to empower entrepreneurs to promote the social good. These crowdfunding sites finance for-profit and non-profit projects:

- 33needs is a crowdfunding site for social enterprises. Its goal is to find businesses that are most able to create change and get them what they need to do it, providing impact investing for social entrepreneurs, social enterprises and companies with a social mission. The social entrepreneurs have between 30-60 days to reach their goal.
- Buzzbnk is an online marketplace that connects social ventures from all walks of life with backers, supporters and fans. Buzzbnk charges a small registration fee for social ventures to join the site.
- CauseVox is a crowdfunding site for both non-profit organizations and for-profit causes. It provides you with a nice set of tools and templates to design your campaign, rally your supports on your website or through social media, track your progress, and utilize your data.
- IndieGoGo offers anyone with an idea — creative, cause-related, entrepreneurial — the tools to build a campaign and raise money. Although this is a general crowdfunding site, it has a clear focus on projects in the public good.

- loby helps you to raise necessary funds and find new volunteers. loby cares about environmental issues in urban neighbourhoods and all the important ways that affect communities.
- OpenIDEO is a social development engine for social change. After a challenge is posted there are three development phases — inspiration, conceptualization, and evaluation. Community members can contribute in a variety of different ways, from inspirational observations and photos, sketches of ideas, to business models and snippets of code.
- Start Some Good is a site for social entrepreneurs to gather a community and raise the funds needed to create change. Both for-profit and non-profit social enterprises can post fundraising campaigns to the site.

Such websites help social entrepreneurs to disseminate their ideas to a broader audience, help with the formation and maintenance of networks of like-minded people and help to link up potential investors, donors or volunteers with the organization. This enables social entrepreneurs to achieve their goals with little or no start-up capital and little or no "bricks and mortar" facilities (e.g., rented office space). For example, the rise of open-source technology as a sustainable tool enables people all over the world to collaborate on solving local problems.

In recent years, much of the emphasis on social enterprise support has been on the early stages of development – from initial concept through to launch and investment. Often termed “incubators” these initiatives typically work with individuals or teams who have an idea for a social enterprise and provide a range of support tools to help them develop and launch it. Some also provide ongoing support for start-ups [4].

## TIPS FOR SOCIAL ENTREPRENEURS:

### ***Take advantage of the resources a co-working space provides***

A lack of office space often prohibits people from starting a business. Co-working spaces solve this problem while giving you a place where you can easily collaborate. Rentals in co-working spaces are cheaper than own office rentals. A possibility is to

search free rentals or even a start-up hub, which can be funded locally, regionally or nationally and provides free offices spaces for start-ups [5].

### ***Use free services to monetize your business***

Social entrepreneurs should promote their businesses through one of the many free services that have recently cropped up. Now there are platforms for every entrepreneur to get out there and be successful without hiring a salesman, designer or a team to build their website. Such websites are online and mobile marketplaces that match freelance labour with local demand, allowing consumers or businesses to find immediate help [5]. Sites that help anyone monetize or sell their skills online: TaskRabbit, Crowdsite, Envato studio, ...

### ***Use crowdfunding***

Social entrepreneurs can also benefit from crowdfunding platforms that give your product a global stage and let the world be your funder. Examples of such platforms and website have been described above [5].

### ***Recognize innovation***

Reading these it means you are a social innovator, nevertheless it is important to boost innovation and to allow anyone in your company to have direct access to the people making the big decisions. Hire great people and give them the chance to innovate. Innovation does not necessarily mean the next big idea; the innovation can be internal the way you communicate or the way your business process works or even the technology you use. In these sense you should consider innovation as anybody or anything that makes your business process better than it was yesterday. In order to become a successful digital social business, it's imperative that all business processes be re-evaluated. If not, there will ultimately be a disconnect in terms of efficiency, access to data and visibility across the end-to-end process – resulting in delays and errors, which are not acceptable in this new digital world [5].

*“Digital technologies open a new and perhaps limitless field of innovative strategies,...” [11]*

***Be a data-driven social entrepreneur***

Making data-driven decisions is key to helping any business grow. Taking advantage of the available data and using it to find out what works best. Small data-driven changes can have a huge impact on the success of a business. It is recommended to use services like Google Analytics for traffic statistics and Google AdWords to help improve SEO on your target market [5].

***Make product advocates part of your team***

Understand who the advocates are and use them to engage with community. Once these influencers are found, one should work hard to keep them engaged. If someone loves a product they will be productive for the venture, making the product a part of their life and sharing it with their friends [5].

Youtubers, vloggers, bloggers are becoming increasingly more important as brand ambassadors for product placement or company advertisement and engage a completely different variety of followers as to your usual target audience. This does not mean you necessarily have to have a brand ambassador it is just a way to engage more and diverse target audience.



## C. Digital Implementation of the Social Entrepreneurship Concept

Social entrepreneurship is an innovative form of entrepreneurship with an emphasis on social solidarity, cooperation and responsible behaviour towards the society and people [6]. Social entrepreneurship has made a strong hold in the business world and has to, as any other business, adapt to the present digital world. The threat lies in the fact that businesses and people involved cannot adapt as quickly to the changes of the digital world and fast as the digital sphere and the technology is changing. Social enterprises are no different in this matter.

In today's ever-changing marketplace we can ask ourselves: How do social businesses survive in the digital age? Most social businesses believe that if they have a website or social media channels it is enough. To have an overall digital marketing presence, one must stand against the competition, and more importantly, drive more customers to their business.

*“Consumer behaviour is evolving at a faster pace than many businesses can cope with. Consistently traditional firms of all sectors are failing to deliver what their customers want and expect in the digital age. And, for those that fail to keep up, the impact can be substantial. With technology changing the way companies operate, there are some significant trends that can help established social companies stay ahead.” [7]*

There is no one-size-fits-all pattern or timetable to creating business changes and adaptations to the digital world, however studies foresee some key steps for companies to consider when adapting to the digital world.

**Communicate the Strategy:** businesses and people cannot change without a sense of purpose, goal and the common understanding and the validation of the communication strategy for the digital economy. The traditional in-office communication does not work if you and your co-workers are entirely digital and communicate via Skype, Viber, e-mails or even through intranet. The communication strategy has to be re-evaluated and adapted to digital environment. By the communication strategy we mean all communication strategies a social business

might have (with consumers, with stakeholders, with co-workers and with all and any other beneficiaries) [8].

**Build New Structures:** Social business working in the digital world might need a different organisational structure than one operating traditionally. As the focus in digital environment has shifted more towards visualisation, photography, video, streaming, social media, one might need more designers, photographers or video editors than in the traditional social business, therefore the organisational structure within the business has to be re-evaluated and designed around the needs of the organisation in the digital environment. These might mean you have to create new structures or teams to support digital operations and business models [8].

**Think Teams:** When brainstorming about any kind of problems or solutions, it is advisable that you include in the think teams employees from different departments, with different skills and in-depth knowledge on policy, communication, analytics, etc. Such different collaboration of people is far more likely to be innovative and agile in searching for a solution [8].

**Experiment and Learn:** Digital innovation means working with and exploiting data in completely new ways. Digital social businesses must adopt a mind-set of speed and experimentation and as a result, you may develop faster responses to consumers and market shifts [8].

**Rethinking IT:** Many IT systems are too slow and rigid for digital business. As companies modernize their IT infrastructure, they are looking to gain flexibility, speed and security [8].

## TIPS FOR DIGITAL IMPLEMENTATION:

- The start-up Power Text Solutions provides a cluster of Web-based individual research tools, such as information categorization and summarization. Its goal is to roll out an unprecedented platform supporting collaborative Web research.
- Google Wave - is intended to allow people from all over the globe to interact, collaborate, and exchange almost any type of information in real time.

## D. Digital Threats and Opportunities for Social Enterprises

The European Commission and the European Economic and Social Committee have addressed the important need for social enterprises to utilise the possibilities of the digitalisation to achieve their social and environmental objectives. “*Social economy and social enterprises must use digitalisation and digital technologies as a lever for economic and social transformation and increased social impact across Europe*” [9].

The opportunity that digital technology offers is far greater for small and medium sized social enterprises and community businesses, often tight on resources. Good digital tools combined with a simple but smart integrated digital and IT strategy enable substantial resource optimisation. “*Make sure that the end goal of implementing a new solution is crystal clear, that you have senior management or trustees' support and that all key stakeholders are involved in the trial of different solutions. Done right, you can save money, time and concentrate on delivering greater impact*” [10].

### Digital Opportunities for Social Enterprises

- + the potential to engage a much larger audience in an interactive environment.
- + social media as reference for personal data (individual's interests, needs, opinions and sentiments).
- + it's a great way to get people talking about your brand cost-effectively.
- + to convey messages for free to a targeted audience.
- + to have an online shop, your customers can be from all over the world [7].

### Digital Threats for Social Enterprises

- time consuming;
- additional staff cost if it is managed internally;

- vulnerable to security breach (sensitive personal or corporate information)
- Fraud/Phishing, Malware/Trojans, Ransomware, Cyber-attacks
- Compliance Pitfalls

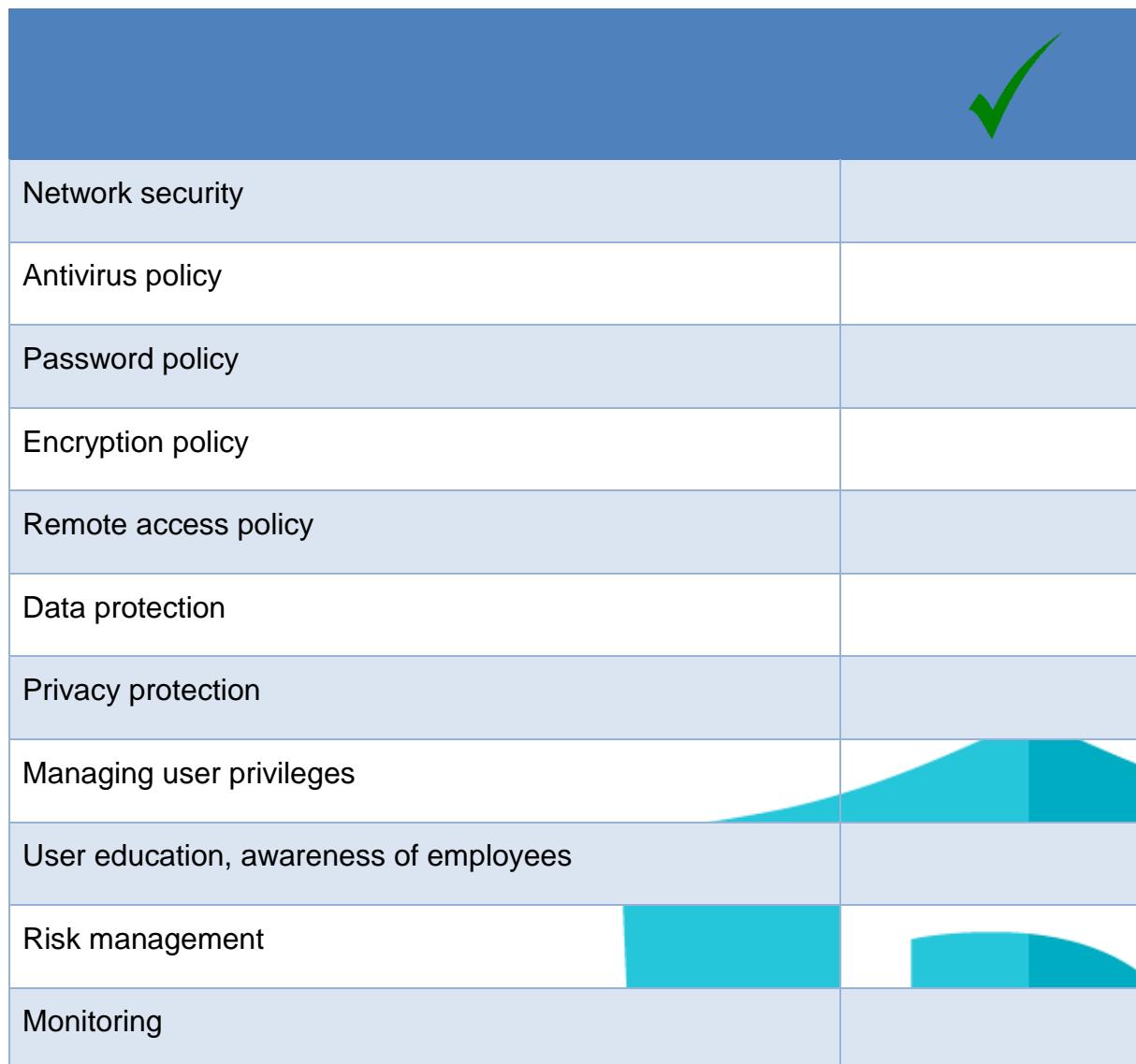
A useful tip when adapting a business to the online environment is to set up an internal business check list. This not only makes it transparent which policies, procedures and processes the organisation went through when adapting to the digital environment, but is also a great and easy way to look at the organisations' weak points as it will be evident what you have neglected or are still in the process of adaptation.

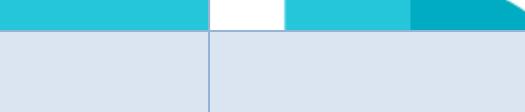
For businesses in a digital environment is important to have an adequate and sufficient hardware but mostly a tight and secure software programmes and applied network securities and policies such as: antivirus, password and encryption. There are many people at different positions working in the organisation who have the access to sensitive or secure information which has to be properly secure, not just only from outside potential hackers but also to prevent any misuse within the organisations' staff. So simple and affective password and encryption policies are recommended for the first steps how to protect ones' information, data and privacy. The organisation or more specifically the director or legal representative has to write down and acknowledge all staff members of their user rights within the system. There has to be a consensus and explanation to which files, information or data specific staff members have access to and to which not. There should also be in place a protocol if a staff member needs specific information that are currently denied by user, privileges what is the procedure for obtaining such information and who is the contact person that approves the privileges upgrade.

High-ranking managers, directors or some significant staff members might have a remote access to the computer servers and to the existing data. Your organisation has to apply a policy where exact staff members are listed and which documents and information are remotely available. All of the above-mentioned steps in the digital security will not function if the organisation has not established a monitoring. If the organisation does not appoint a clear monitoring system with a specific staff member

in charge and if the penalties for any kind of violation are not known to everybody, the checklist of the threats is pointless.

## E. Digital Security Checklist



	
Network security	
Antivirus policy	
Password policy	
Encryption policy	
Remote access policy	
Data protection	
Privacy protection	
Managing user privileges	
User education, awareness of employees	
Risk management	
Monitoring	

## F. Terminology glossary

**Crowdsourcing** - is a sourcing model in which individuals or organizations obtain goods and services, including ideas and finances, from a large, relatively open and often rapidly-evolving group of internet users; it divides work between participants to achieve a cumulative result. As a mode of sourcing, crowdsourcing existed prior to the digital age (i.e. "offline").

**Digital Entrepreneurship** – Digital entrepreneurship may be defined as entrepreneurship in which some or all of the entrepreneurial venture takes place digitally instead of in more traditional formats. Products, distribution, the workplace-any of these and more could take digital form in an entrepreneurial venture.

**Digital marketplace** - The internet makes available huge assortment of products and services to everyone on the planet with an internet connection. For digital products like music or software, the distribution of a product becomes instantaneous and free. With the introduction of a website, any venture instantly goes global.

**Digital workplace** - The reach of the Internet allows digital entrepreneurs to take advantage of potential employees and partnerships all over the globe without forcing anyone to relocate. Global virtual teams can offer considerable benefits to the digital entrepreneur, making it easy to locate and hire talent, harnessing cultural diversity, improving resource utilization and increasing flexibility and responsiveness.

**Open source software** – computer software with a source code that can be seen, modified and distributed freely. Open source software is generally considered a safer alternative than proprietary software because developers can test it to detect any backdoors.

**Ransomware** is a type of malicious software from crypto virology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

**Spyware** – software that collects information about your computer and how you use it and then relays that information to someone else over the Internet. Spyware ordinarily runs in the background and often installs itself on your computer without your knowledge or permission.

**Virus** – a program or code that replicates itself onto other files with which it comes into contact. Most viruses only replicate, although many can do damage to a computer system or a user's data as well.



## G. Conclusions and Further Reading

Social businesses have to adapt to the demands of ever-changing digital economy for it to stay present and operational. Ever changing digital environment and the progress of technology are becoming a vital aspect of businesses were sources and resources have to be allocated faster than other business aspects. Some social businesses have made these progress and transition with little or no investments or efforts while other businesses need additional help. The digital environment is forcing social businesses to re-evaluate the business strategies they might have and modify them to the current digital environment. This also includes evaluation of all business processes that were established before the transition. With rethinking and re-defining new strategies, some businesses might experience a shift also in organisational staff structures. Mobility and flexibility are crucial for employees to remain relevant in the digital economy. To sustain a digital transformation, businesses have to adopt new technologies, new business processes and pay extra attention to supporting systems and security. Nevertheless, businesses cannot change, modify or adapt only hardware systems and processes without changing the people. If the workplace is changing, the workforce also has to.

Some further reading into the topic:



The impact of the  
digital world on  
management and  
marketing

**KOZMINSKI  
UNIVERSITY**

New technologies and  
digitalisation:  
opportunities and  
challenges for social  
economy and social  
enterprise

**EECS**

Boosting Social  
Enterprise  
Development: Good  
Practice Compendium

**OECD**

## H. References

- [1] OECD, 2016 Ministerial meeting: Managing Digital Security and Privacy Risk for Economic and Social Prosperity, <https://www.oecd.org/internet/ministerial/meeting/Managing-Digital-Security-and-Privacy-Risk-discussion-paper.pdf>
- [2] Growing a Digital Social Innovation Ecosystem for Europe (2015), European Union, <https://www.nesta.org.uk/sites/default/files/dsireport.pdf>
- [3] Durieux, Mark and Stebbins, Robert (2010): Social Entrepreneurship for Dummies, Wiley Publishing, Inc., Hoboken, <http://socialnaekonomija.si/wp-content/uploads/2015/03/Social-Entrepreneurship-For-Dummies-Mark-Durieux.pdf>
- [4] British council (2015): Social Enterprise in the UK – Developing a thriving social enterprise sector, [https://www.britishcouncil.org/sites/default/files/social\\_enterprise\\_in\\_the\\_uk\\_final\\_web\\_spreads.pdf](https://www.britishcouncil.org/sites/default/files/social_enterprise_in_the_uk_final_web_spreads.pdf)
- [5] Rupa Rathee (2017): ENTREPRENEURSHIP IN THE DIGITAL ERA, Asia Pacific Journal of Research in Business Management, Vol. 8, Issue 6, June 2017 Impact Factor: 5.16, ISSN: (2229-4104), [https://www.academia.edu/33640590/ENTREPRENEURSHIP\\_IN\\_THE\\_DIGITAL ERA?auto=download](https://www.academia.edu/33640590/ENTREPRENEURSHIP_IN_THE_DIGITAL ERA?auto=download)
- [6] Socialno podjetništvo za začetnike, Ljubljana: ŠOU
- [7] Rossi, Ben (2016): How companies must adapt to the digital revolution, <http://www.information-age.com/how-companies-must-adapt-digital-revolution-123461760/>
- [8] Harward Business Review, Is Your Company Adapting Fast Enough to Thrive in an Increasingly Digital World?, October 2017, <https://hbr.org/sponsored/2017/10/is-your-company-adapting-fast-enough-to-thrive-in-an-increasingly-digital-world>
- [9] New technologies and digitalisation: opportunities and challenges for Social Economy and Social Enterprise, <https://www.eesc.europa.eu/en/agenda/our->

[events/events/new-technologies-and-digitalisation-opportunities-and-challenges-social-economy-and-social-enterprise](#)

[10] Violo, Marc (2017): Digital Tool Box for Social Enterprises & Charities,  
<https://medium.com/on-purpose-stories/digital-tool-box-for-social-enterprises-charities-b4bc3f4c4184>

[11] Prodanov, Hristo (2018): Social Entrepreneurship And Digital Technologies, Economic Alternatives, 2018, Issue 1, pp. 123-138,  
[https://www.unwe.bg/uploads/Alternatives/9\\_Prodanov\\_EAlternativi\\_en\\_1\\_2018.pdf](https://www.unwe.bg/uploads/Alternatives/9_Prodanov_EAlternativi_en_1_2018.pdf)



# **SECTION III**

## **LEGAL ISSUES REGARDING DIGITAL SECURITY**



## List of abbreviations

Abbreviation	Definition
EU	European Union
GDPR	General Data Protection Regulation 2016/679
CRD	Consumers Right Directive 2018/83
EPD	e-Privacy Directive
HTTP	Hypertext Transfer Protocol
MS	Member State



## A. Introduction

The creation of a true, properly working Digital Single Market with a resilient European Data Economy is one of the main priorities of the European Union. This means that essentially an effective cross-border free flow of data should be in place. European companies are also increasingly picking up on digital developments and are beginning to incorporate digital business models to make full use of data and data analytics.

The proper functioning of network and information systems all over the EU is essential to keep the online economy running and to ensure prosperity. To this end, the EU works on a number of fronts to promote cyber resilience.

But these new business models do not exist “out in the wild”. In order to really benefit from them, one should take into account the application regulatory regime. In the current chapter, you will get acquainted with the European legal framework related to digital security. The first part of the chapter is dedicated to the most recent changes in the EU legislation which caused turbulences in the European society – namely the General Data Protection Regulation (GDPR). The thorough analysis of the Regulation is followed by an overview of the Consumer Rights Directive (CRD), the e-Commerce Directive and the e-Privacy Directive (EPD).



## B. Data Protection Guidelines

As of May 25th, 2018, there are new legal requirements for companies that process personal information.

You may have heard of the General Data Protection Regulation 2016/679, also known as GDPR. It is an EU regulation, which applies to any company doing business with customers in the EU, offering goods or services on EU territory, and dealing with data, related to EU citizens, including its employees. The main purpose of GDPR is to protect EU residents' personal data through strict requirements impacting the entire data lifecycle within most organisations. As it is the major set of rules and regulations that governs the use of personal data within the EU, GDPR is of huge importance for the majority of businesses in the region.

How important GDPR is for the business can be seen in the fines, foreseen for failing to comply. For non-compliance, organisations, even if they're not based in the EU, can face up to EUR 20 million in fines, or 4% of their total global revenue for the preceding fiscal year - whichever is higher. This means that if a company has customers or employees in the EU, the GDPR requirements must be taken seriously.

To avoid these fines, you as an entrepreneur or as a part of a company should seek compliance with GDPR requirements on the following, which will be discussed in detail below:

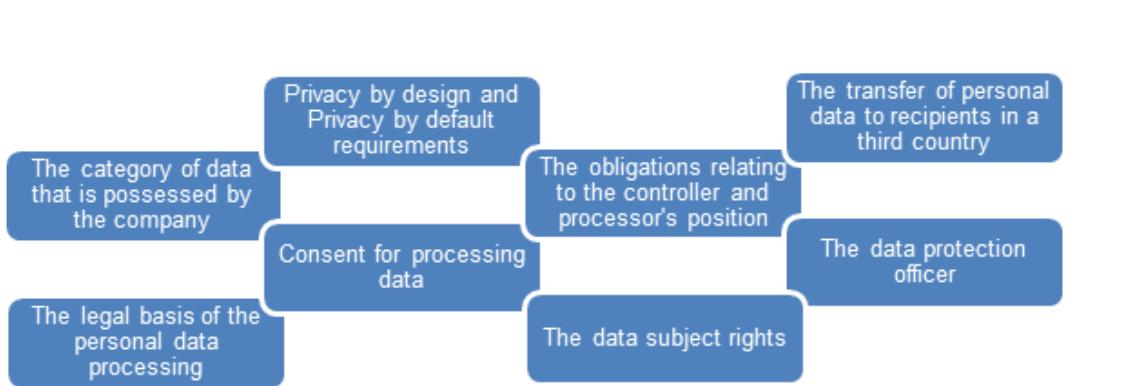


Figure 1: Areas in which to seek GDPR compliance

### Personal data

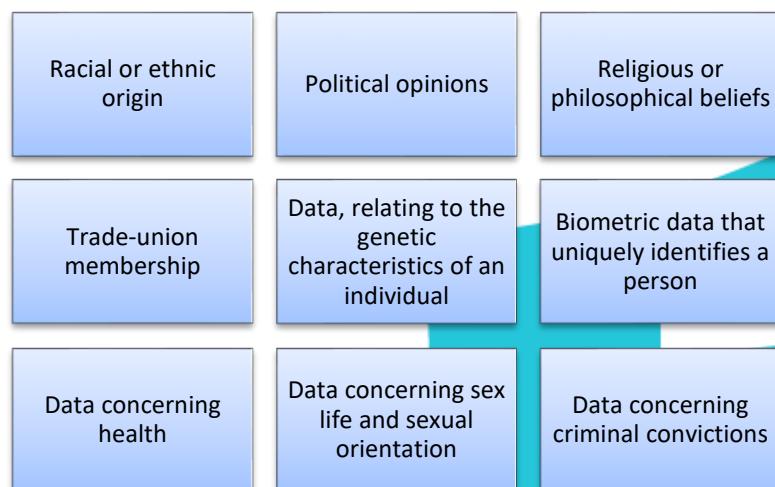
First of all, in order to attain compliance with GDPR, it is of great importance to understand to which information - or data - GDPR refers to and protects – namely, what is personal data.

First: personal data is not data that relates to a legal person and is not data of a deceased person.

Personal data means any information relating to a data subject, who is either:

- an *identified* natural person – a person who can be distinguished from other members of a certain group, for example by name or a photo;
- an *identifiable* natural person – a person who can be directly or indirectly identified, for example, based on information that makes the identification of a person by reasonable means possible, such as his/her voice or his IP address.

Special categories of personal data, often referred to as 'sensitive data', include personal data revealing:



**Figure 2: Special categories of personal data**

On principal, it is prohibited to process these special categories of data, unless the data subject gives their explicit consent, or the processing relates to personal data which are manifestly made public by the data subject, or you are required by law to process such personal data. This includes, in most cases, health records of persons.

In terms of employment, there are some exceptions since employers have the right (if necessary) to process sensitive data of employees. However, you, as an employer,

should make sure that you do not keep sensitive information, which permits identification of employees, for longer than is reasonable, and you should not base any decision purely on automated processes and evaluations (including profiling).

An important subcategory of personal data is Pseudonymised data, which is data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is secured and stored separately. In other words, this is personal data, which is related to an identifiable natural person through reasonable means (which is determined by costs and amount of time needed for identification, as well as available technology at the time of the processing). Pseudonymisation is a way to mitigate the risks, related to processing personal data.

On the other hand, anonymous information is that, which cannot identify the data subject in any way – and its processing is not regulated by GDPR. An important note: data can only be considered anonymous if re-identification is virtually impossible, meaning that re-identifying an individual must be impossible by any party and by all means likely reasonably to be used for this attempt.

More practical information on how to pseudonymise and anonymise data is available in Section IV and V of this e-Manual.

## Processing

To comply with GDPR, you should know what constitutes processing of personal data. According to the Regulation, processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as **collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction**.

This applies to all wholly or partially automated systems, and even to fully non-automated means, which form part of a filing system or are intended to form part of a filing system. The definition of a “filing system” is given within GDPR and means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or

geographical basis. An example of that filing system could be even the business cards you get from partners: collecting them in a card holder is creating a filing system.

What should be also clarified is that the processing of personal data by a natural person in the course of a **purely personal or household activity** and thus **with no connection to a professional or commercial activity**, is not covered by GDPR. For example, even corresponding in Facebook is considered processing of personal data, however since it is only for personal use and with no commercial goal, it is not controlled by GDPR. However, when you communicate with people in social media but for commercial purposes (i.e. selling products on Instagram), GDPR applies.

	YES	NO
<b>Is the data relating to a natural person?</b>	GDPR applies ✓	GDPR does not apply ✗
<b>Does this data in some way identifies a natural person?</b>	GDPR applies ✓	GDPR does not apply ✗
<b>Can I separate or segregate that identifiable data from what is left over?</b>	GDPR does not apply ✗	GDPR applies ✓
<b>Do I plan to in some way monetise this data?</b>	GDPR applies ✓	GDPR does not apply (in personal or household activities) ✗

Figure 3: Summary of GDPR application

## Basic principles of processing

According to GDPR, any kind of processing of personal data and is covered by the Regulation has to be compliant with the following principles:

- |                     |  |
|---------------------|--|
| <b>Lawfulness</b>   | - Process data on the legal grounds listed in Art. 6 GDPR;   |
| <b>Fairness</b>     | - Inform data subject of existence and nature of processing;   |
| <b>Transparency</b> | - Make information on processing of personal data easily accessible and easy to understand (incl. information about identity of data controller & purposes of processing, and risks, rules, safeguards, rights related to processing);<br>- Inform data subject of the existence of profiling and its consequences;<br>- Inform data subject whether they are obliged to give personal data and what are the consequences. |

<b>Specified Explicit Purposes</b>	- If personal data is processed on the basis of legitimate purpose, state in specified and explicit way what is this legitimate purpose at the time of the collection;
<b>Legitimate</b>	- Do not further process available data when incompatible with those purposes; - When the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject (prior to the further processing) with information on what the other purpose is and other necessary information; - This new processing should adhere to all principles again.
<b>Data minimisation</b>	- The collected personal data must be adequate, relevant and limited to what is strictly necessary in relation to the purposes of the processing;
<b>Storage limitation</b>	- The personal data is to be kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data is processed (exempt is keeping information for archiving purposes in the public interest, scientific or historical research or statistical purposes, supplemented with specific measures to safeguard

	<p>the rights and freedoms of data subjects).</p>
<b>Accuracy</b>	<ul style="list-style-type: none"><li>- The personal data must be accurate and, where necessary, kept up to date;</li><li>- With reasonable means, make sure to rectify or erase in a timely fashion all inaccurate personal data.</li></ul>
<b>Integrity</b> <b>Confidentiality</b>	<ul style="list-style-type: none"><li>- Ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage;</li><li>- Ensure that the processed personal data is protected from any potential leaking as well as the personal data will not be lost, destructed or damaged;</li><li>- In case of an incident, which breaches the abovementioned, the controller is liable for the damage caused and can be asked for compensation if they cannot prove that they are not in any way responsible for the damage and that all appropriate technical and organisational measures to protect the database has been implemented;</li><li>- To ensure an appropriate level of security, make sure to:<ul style="list-style-type: none"><li>o pseudonymise and encrypt personal data;</li><li>o ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;</li><li>o arrange for the ability to restore availability and access to data in a timely manner in the event of an incident;</li><li>o regularly test, assess and evaluate the effectiveness of technical and organizational security measures.</li></ul></li></ul>
<b>Notification to the supervisory authority</b>	<ul style="list-style-type: none"><li>- Personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Can be any single or combination of:<ul style="list-style-type: none"><li>o “Confidentiality breach” - an unauthorised or accidental disclosure of, or access to, personal data;</li><li>o “Availability breach” - an accidental or unauthorized loss of</li></ul></li></ul>

	<p>access to, or destruction of, personal data;</p> <ul style="list-style-type: none"><li>○ “Integrity breach” - an unauthorised or accidental alteration of personal data;</li><li>- The data breach notification to the competent supervisory authority (data protection authority) should be done no later than 72 hours after being aware of it;</li><li>- It is necessary that the data protection authority is provided with information on: the nature of the breach; categories and approximate number of data subjects and records concerned; name and contact details of the Data Protection Officer; likely consequences of the breach; measures taken on proposed. If there is a delay in reporting, the delay should be justified;</li><li>- Breaches that are unlikely to result in a risk to the data subjects do not require reporting to the supervisory authority (for example publicly available personal data, or hashed and salted data, which still has a non-compromised key).</li></ul>
<b>Communication to the data subject</b>	<ul style="list-style-type: none"><li>- Where there is a high chance of adverse effects arising from a data breach, the data breach should be communicated to the affected individuals as soon as reasonably feasible;</li><li>- Provide specific information about the likely consequences and the steps they should take to protect themselves, as well as a description of the nature of the breach, name and contact details of the Data Protection Officer or another contact point;</li><li>- Keep communication clear and transparent, without including other information like regular updates, newsletters, etc.;</li><li>- Use more than one communication channel (SMS, e-mail, website banners, prominent advertisements, etc.) to effectively reach the affected individuals;</li><li>- No notification is required if all three conditions below are met:<ul style="list-style-type: none"><li>○ If data is unintelligible to any person not authorised to access it (for example, if it is encrypted securely);</li><li>○ Immediately after a breach, the necessary steps are taken to ensure that the risk is no longer likely to materialise;</li><li>○ It would involve disproportionate effort to contact individuals</li></ul></li></ul>

	(if their contacts were lost or were not known in the first place).
<b>Risk and High risk</b>	<ul style="list-style-type: none"> <li>- After a breach, it is important to assess the risk that could result from it, so the likelihood and severity of impact on the individuals are known, as well as if a notification is required;</li> <li>- Risk exists when the breach may lead to physical, material or non-material damage for the individuals, whose data have been breached;</li> <li>- Criteria to take into account: <ul style="list-style-type: none"> <li>o The type of breach;</li> <li>o The nature, sensitivity, and volume of personal data;</li> <li>o Ease of identification of individuals;</li> <li>o Severity of consequences for individuals;</li> <li>o Special characteristics of the individual;</li> <li>o The number of affected individuals;</li> <li>o Special characteristics of the data controller.</li> </ul> </li> </ul>
<b>Accountability</b> <b>Record keeping</b>	<ul style="list-style-type: none"> <li>- Regardless of the need for notification, the controller must keep documentation of all breaches;</li> <li>- It is recommended to establish an internal register of breaches, which includes causes, description, effects, remedial action taken;</li> <li>- It is recommended to create and keep a procedure, which includes how to contain, manage and recover incidents, assessing risks and required notifications, and inform employees of the procedure.</li> </ul>

**Figure 4: Basic principles of data processing**

## C. Consumer Protection Guidelines

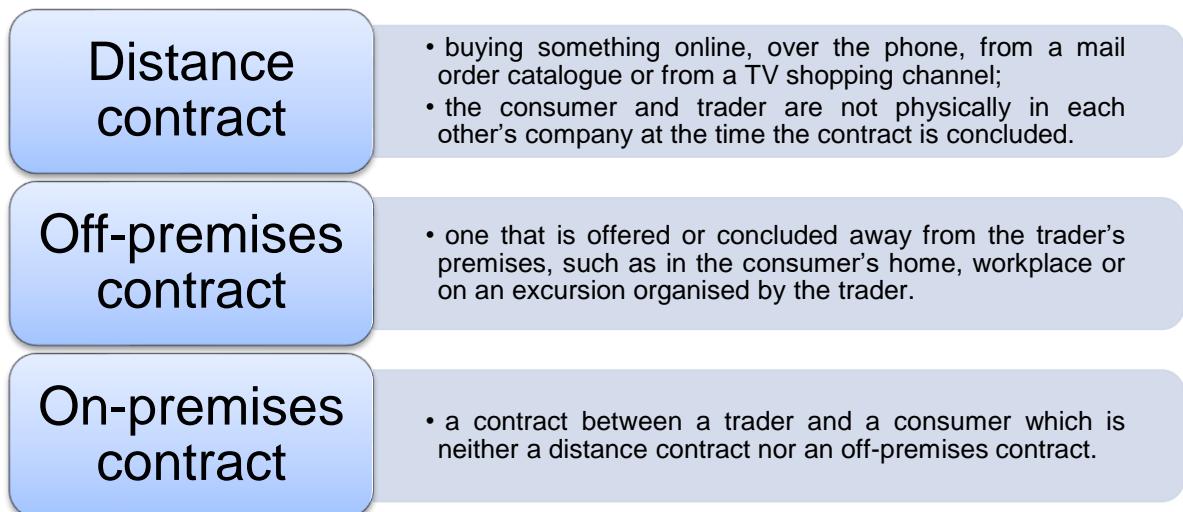
Similar to how data protection is governed by GDPR, consumer protection is governed by the EU Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights (also known as Consumer Rights Directive). It replaces two previous Directives – one (Council Directive 85/577/EEC) on consumer protection in respect of contracts negotiated away from business premises and one (Directive 97/7/EC of the European Parliament and of the Council) on the protection of consumers in respect of distance contracts.

The purpose of the Directive is to achieve a high level of consumer protection across the EU and to contribute to the proper functioning of the internal market. The Directive applies to any contract concluded between a trader and a consumer.

Member States (MS) were required to implement it into their national law by 13 December 2013, and all national transposition measures are set in place from 13 June 2014.

The Directive is implemented with maximum harmonisation, also known as “full harmonisation”, meaning that the MSs could not adopt more restrictive rules in the area – the rules in the Directive are the maximum applicable. The Directive establishes certain key consumer rights and sets out rules on contracts between consumers and businesses, which has a direct tangible effect on the everyday life of consumers across the EU.

The types of contracts distinguished by the Directive are three: off-premises contracts, distance contracts and on-premises contracts.



**Figure 5: Different contracts according to Directive 2011/83/EU**

The Directive further categorises contracts into four categories: sales contracts, service contracts, contracts for online digital content and contracts for the supply of public utilities. Classifying a contract as either a “sales” or a “service contract” determines how the withdrawal period is calculated (Article 9). The withdrawal period is defined as the period when a customer can terminate the contract without giving a reason and without the burden of any additional costs. For service contracts, digital content and contracts for the supply of public utilities, the 14-day withdrawal period starts running from the conclusion of the contract. For sales contracts, the withdrawal period only starts running after the goods are received.

Specifically, regarding digital goods, anyone buying digital content must be able to get clear and unambiguous information, including details on the software and hardware the content works with, as well as information on copyright, according to the Directive. Consumers must be able to pull out of purchases of digital content up to the point where downloading or streaming of the content begins.

The Directive excludes certain categories of contracts from its application, including:



**Figure 6: Categories of activities, excluded from the Consumer Rights Directive**

## Consumer Rights Directive in a nutshell

The purpose of the Directive is to achieve a high level of consumer protection across the EU and to contribute to the proper functioning of the internal market by approximating certain aspects of MSs' laws, regulations and administrative provisions concerning contracts concluded between consumers and traders.

What the Directive means for businesses and consumers is summarised in the table below:

Advantages for consumers	<ul style="list-style-type: none"><li>- The information that consumers must be provided with before purchasing something and the right of the consumers to cancel online purchases is now the same in all EU countries;</li><li>- Consumers can rely on the same rights, wherever they shop in the EU;</li><li>- Stronger consumer rights and higher level of protection regardless of place and manner of shopping;</li><li>- Full information on the total cost of the product</li></ul>
--------------------------	--

	<b>or service, including any extra fees (e.g. delivery costs).</b>
New rules for the business	<ul style="list-style-type: none"><li>- No more cost-traps on the Internet: online shoppers need to confirm that they accept paying for something before they are charged (the price should be clearly indicated). The customers do not have to pay for any charges of which they are not clearly informed before making the purchase;</li><li>- No more pre-ticked boxes: a clear ban is introduced by the Directive for the pre-ticked boxes on websites that are charging additional payments;</li><li>- Traders are not be allowed to charge more for credit card payments than it costs them to provide such a payment option;</li><li>- The rates for hotlines for customer complaints or questions should be no more than the basic rate for such calls.</li></ul>
	<b>Refund rules:</b> <ul style="list-style-type: none"><li>- The period for consumers to pull out of any distance purchase (e.g. online) or off-premises purchase (when a seller visits the consumer's home) is extended from the previous minimum 7 days, to a uniform 14 day across the EU;</li><li>- The 14 days start counting from the day the consumer receives the goods, and the consumer has the right to cancel the purchase for any reason. When a seller hasn't clearly informed the consumer about the right to cancel the purchases, the return period is extended to a year;</li><li>- Traders must refund consumers within 14 days of cancellation, including the standard delivery cost. Regarding goods, the trader can postpone the</li></ul>

	<p>reimbursement until the goods are returned by the consumer or the consumer provides evidence that these goods have been sent to the trader. This does not apply for custom made products or for perishable products (such as dairy products);</p> <ul style="list-style-type: none"><li>- Consumers are given a standard EU form to use if they want to cancel their purchases, although they are not obliged to use it. If the traders want the consumer to pay for the return of goods after cancellation, they must clearly inform them before and give at least an estimate cost for returning.</li></ul>
Important implications for the business	<ul style="list-style-type: none"><li>- Common rules for businesses make trade all over Europe easier;</li><li>- Businesses making sales by phone, mail or online, or away from their premises, have a single set of rules to follow. This creates a level playing field and cuts cross-border transaction costs;</li><li>- With regards to small businesses and craftsmen, there is no right to pull out of a contract for urgent repairs and maintenance jobs. Member States can also exempt traders doing repairs or maintenance jobs in customers' homes for less than EUR 200 from certain information requirements.</li></ul>

Figure 7: Implications from the Consumer Rights Directive

## Compliance with the Directive for businesses

In order to be compliant with all aspects of the Directive, here are some useful tips, which will also be summarised in the complete Legal checklist at the end of this part of the e-Manual.

- 1) Make sure your website has Terms and Conditions, which inform your customers of all their relevant rights and obligations. Some of that information should also be included in Order policies or at the pages, which customers use to order your products or services. Include information on returns, cancellations, refunds, etc.
- 2) When any changes are made in the Terms and Conditions, make an effort to let your customers know. For example, after Airbnb.com changed their Terms in June of 2017, the users of their services received this e-mail:



Our community and vision for travel have grown significantly, so we're updating our Terms of Service, Payments Terms of Service, and Privacy Policy (collectively, "Terms"). Also, we rewrote and restructured the Terms to make them shorter, more concise, and easier to read. The changes will go into effect for all existing users on August 25, 2017. When you use Airbnb on or after that day, we'll ask you to agree to the new Terms.

You can review the new Terms by clicking [here](#). We've also put up information to explain these changes in more detail on our [Terms of Service Update page](#). Both the old and new versions of the Terms can be found at the [Terms of Service](#), [Payments Terms of Service](#), and [Privacy Policy](#), tabs through September 25, 2017. You should review these Terms in full yourself.

Thank you for being a member of our global community.

- 
- 3) Create a way for your customers to show that they understand their rights and obligations – that usually happens with a box to be ticked before registration or before finalisation of an order.
  - 4) Related to the previous point, remember that pre-ticked boxes are completely forbidden.
  - 5) Make sure the customers can get in touch with you without having to incur any additional charges (premium rate lines, etc.).

- 6) Provide an easily-accessible cancellation form for your customers.



## D. e-Commerce Guidelines

In the way data protection is governed by GDPR and consumer protection is governed by the EU Directive 2011/83/EU, electronic commerce (e-commerce) is governed by Directive 2000/31/EO of the European Parliament of the Council of 8 June also known as the e-Commerce Directive.

MSs were required to transpose it into their national laws by 17 January 2002. The objective of the Directive is to create a legal framework to ensure the free movement of information society services between MSs. It establishes standard rules in the EU on various issues related to e-commerce. This Directive approximates certain national provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions and cooperation between Member States.

		Does the Directive apply?
News services (such as news websites)		✓
Selling (books, financial services, travel services, etc.)		✓
The field of taxation		✗
Advertising		✓
Professional services (lawyers, doctors, estate agents)		✓

Gambling activities which involve wagering a stake with monetary value in games of chance, including lotteries and betting transactions.	X
The activities of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority,	X
Entertainment services	✓
Questions relating to information society services	X
Basic intermediary services (internet access, transmission and hosting of information)	✓
Free services funded by advertising, sponsorship, etc.	✓
Questions relating to agreements or practices governed by cartel law	X

**Figure 8: Application of the e-Commerce Directive**

### **Liability of intermediaries**

The e-Commerce Directive contains several provisions on the liability of intermediaries. It establishes harmonised rules on issues such as transparency and information requirements for online service providers, commercial communications, electronic contracts and limitations of liability of intermediary service providers.

### **“Mere Conduit”**

Service providers, whose role solely consists in the transmission of information originating from third parties and the provision of access through a communication network, cannot be held liable for third party illegal content if they:

- Do not initiate the transmission;
- Do not select the receiver of the transmission; and
- Do not select or modify the information transmitted.

Automatic, intermediate and transient storage of information which takes place during the transmission of the information in order to carry out the transmission, are covered by the exemption of liability.

### **“Caching”**

Service providers cannot be held liable for third party illegal content when providing caching facilities provided they:

- Do not modify the information;
- Comply with conditions on access to information and with rules on the updating of the information;
- Do not interfere with lawful use of technology to obtain data on the use of the information;
- Expediently act to remove the access to the information stored when informed that the information has been removed from the network, when access to it has been disabled or when a responsible authority has ordered the removal.

### **“Hosting”**

Service providers who store information supplied by and at the request of a recipient of the service are not liable if:

- They do not have actual knowledge of illegal activity or information and as regards claims for damages and are not aware of the facts or circumstances from which the illegal activity or information is apparent; or
- The provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the information.



## E. Cookies

### What are Cookies?

An HTTP cookie also referred as web cookie, Internet cookie, browser cookie, magic cookie, or simply cookie is a small piece of data which are stored on a user's computer or mobile phone and can be read with Notepad. The cookie allows the website to "remember" your actions or preferences over time (for example if you've placed items in your online basket, you can access them in your next visits on the website). The can also record user's activity, including clicking buttons history, logging in information, names, addresses, passwords, etc. Most browsers support cookies, but users can decide whether they accept them and delete them whenever they like.

### Different types of cookies

There are two basic type of cookies classified by its lifespan and the domain to which they belong. They are:

- **Session cookies** (in-memory cookie, transient cookie or non-persistent cookie) exist only in the temporary memory while the user navigates the website. They are usually deleted when the user exits the browser.
- **Persistent cookies** expire on a specific date or after a specific length of time unlike the session cookies depending on the wishes of the creator. The information they contain is transmitted to the server every time the user visits the website that they belong to. They are referred also as tracking cookies because they can be used by advertisers to record information about the user's browsing habits.

As for the domain to which they belong, there are divided into:

- **First-party cookies** which are set by the web server of the visited page and share the same domain meaning that the cookie's domain attribute will match the domain that is shown in the web browser's address bar.

- **Third-party cookies** stored by a different domain to the visited page's domain. This sort of cookie typically appears when web pages feature content from external websites, such as banner advertisements. This opens up the potential for tracking the user's browsing history and is often used by advertisers in an effort to serve relevant advertisements to each user.

There are also *secured cookies*, *http-only cookies*, *supercookies*, *zombie cookies*.

Under normal circumstances, cookies cannot transfer viruses or malware to your computer. Because the data in a cookie doesn't change when it travels back and forth, it has no way to affect how your computer runs. However, some viruses and malware may be disguised as cookies. For instance, "supercookies" can be a potential security concern, and many browsers offer a way to block them. A "zombie cookie" is a cookie that recreates itself after being deleted, making zombie cookies tough to manage. Third-party tracking cookies can also cause security concerns, since they make it easier for parties you can't identify to watch where you are going and what you are doing online.

## The e-Privacy Directive

The use of cookies brings privacy concerns. In May 2011, an EU Directive was adopted to protect consumer privacy online. That is Directive 2009/136/EC that became known as the Cookie Law - e-Privacy Directive. It is applicable to any person or organisation that is physically located in the EU and has a website and / or any website that targets EU consumers, and the website is using cookies.

The legislation requires that the covered websites:

- ✓ Let users know if they are using cookies;
- ✓ Explain what data is gathered with cookies and how data is used;
- ✓ Gather user consent to use of cookies.

If you own a website, you will need to make sure it complies with the law, and this usually means making some changes. Compliance with the e-Privacy Directive comes down to three basic steps:

- ✓ Let users know that you are using cookies;
- ✓ Provide a link where they can learn more about how you use the data gathered;
- ✓ Provide a way for users to consent to the use of cookies.

The most common way to do this is to display a small banner at the top or bottom of your website with a link to a detailed privacy/ data protection policy and a button to consent to the use of cookies and hide the banner.

There are two types of consent that websites can gather:

- **Explicit opt-in consent** - users have to click a button, select a checkbox, or complete some other specific activity to opt-in to the use of cookies. When explicit consent is gathered, there's no way for users to accidentally consent to the use of cookies
- **Implied consent** - one common way that implied consent is gathered is to display a prominent cookie notice that ends with a statement like: "*By continuing to use this site you agree to the use of cookies.*" It is important that a clear notice is provided, and the user is aware that some other specific action will be understood as implied consent to the use of cookies.

The legislation applies whether a user is on a computer, smartphone, tablet, or any other device. Therefore, when you set up a cookie notice it's important to make sure that the notice appears and functions appropriately on all devices.

## GDPR and Cookies

The purpose of GDPR is to protect "*natural persons with regard to the processing of personal data and on the free movement of such data*", in other words the website users. Cookies are mentioned once in Recital 30 of GDPR. However, these lines have a significant impact on the compliance of cookies:

(30)

*Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie*

*identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.*

In other words, when cookies can identify an individual, it is considered personal data.

Not all cookies are used in a way that could identify users, but the majority are and will be subject to the GDPR. This includes cookies for analytics, advertising and functional services, such as survey and chat tools.

To become compliant, organisations will need to either stop collecting the offending cookies or find a lawful ground to collect and process that data. Most organisations rely on consent (either implied or opt-in), but the GDPR's strengthened requirements mean it will be much harder to obtain legal consent.

- **Implied consent is no longer sufficient.** Consent must be given through a clear affirmative action, such as clicking an opt-in box or choosing settings or preferences on a settings menu. Simply visiting a site doesn't count as consent.
- **'By using this site, you accept cookies' messages are also not sufficient for the same reasons.** If there is no genuine and free choice, then there is no valid consent. You must make it possible to both accept or reject cookies. This means:
  - **It must be as easy to withdraw consent as it is to give it.** If organisations want to tell people to block cookies if they don't give their consent, they must make them accept cookies first.
  - **Sites will need to provide an opt-out option.** Even after getting valid consent, sites must give people the option to change their mind. If you ask for consent through opt-in boxes in a settings menu, users must always be able to return to that menu to adjust their preferences.

## F. Legal Compliance Checklist



<b>My website includes:</b>	
Terms and Conditions	
Rights and Obligations	
NO pre-ticked boxes	
FREE Contact	
Cancellation Form	
I do not keep sensitive data for no longer than is reasonable	
I know what constitutes processing of personal data	
<b>When processing personal data, I am compliant with the principles of:</b>	
Lawfulness	
Fairness and Transparency	
Legitimacy	
Data minimisation and storage limitation	
Accuracy	
Integrity and confidentiality	
Notification to the supervisory authority	
Communication to the data subject	

Risk and High Risk	
Accountability and Record keeping	
The service/product I provide contains full information on the total cost, including any extra fees	
I do not charge more for credit card payments	
The hotline for my customers is set up on the basic rate	
I let users know if they are using cookies	
I gather user consent to use cookies	
I explain what data is gathered when giving consent to using cookies	



## G. Terminology glossary

**EU Regulation** - A regulation is a legal act of the EU that becomes immediately enforceable as law in all member states simultaneously.

**EU Directive** - A directive is a legal act of the EU which requires MSs to achieve a particular result without dictating the means of achieving that result. It can be distinguished from regulations, which are self-executing and do not require any implementing measures. Directives normally leave MSs with a certain amount of leeway as to the exact rules to be adopted. Directives can be adopted by means of a variety of legislative procedures depending on their subject matter.

**Transposition measures** - In EU law, transposition is a process by which the EU's member states give force to a directive by passing appropriate implementation measures. Transposition is typically done by either primary or secondary legislation.

**Internal market** – Also known as the European Single Market or Common Market, the Internal market is a single market which seeks to guarantee the free movement of goods, capital, services, and labour – the "four freedoms" – within the EU.

**Compliance** – Conforming to the existing legislation, be that national or international.



## H. Conclusions and Further Reading

This Chapter of the e-Manual described in detail necessary information about the General Data Protection Regulation (GDPR, followed by an analysis on Consumer Rights Directive (CRD), the e-Commerce Directive and the e-Privacy Directive (EPD).

Based on the discussed topics and after going through the checklist, your business is now compliant to EU regulations. It is important to never overlook what EU and national regulations point at in terms not only of being safe from fines but also being a socially responsible business.

Legal advice is often seen as expensive and hard to acquire, however make sure to consult with people, who are aware of what businesses need in order to be compliant and avoid going around some rules for cutting some expenses – these ‘loopholes’ may cost you much more in the future!

For some free mentoring and advice on the topic, you can use the DiFens mentoring platform, available at <http://www.difens.eu/>, where legal experts can also assist in your specific case.

Some other further reading:

Are you ready for  
tomorrow's data  
compliance  
challenges?

**FORBES**

Is your website legal?

**YFS Magazine**

The lifecycle of data  
protection is evolving.  
Here's what you need  
to know.

**FORBES**

Legal regulations for  
e-commerce

**EUROPEAN  
COMMISSION**

Summary of adoption  
of e-commerce  
legislation worldwide

**UNCTAD**

Why cookie  
alternatives are vital  
for the future of mobile  
advertising?

**CLEARCODE**

## I. References

Competition and Consumer Protection Commission (2017) The Consumer Rights Directive: A guide for traders dealing with consumers. Available from: [https://www.ccpc.ie/business/wp-content/uploads/sites/3/2017/03/CRD-Guidance\\_FINAL.pdf](https://www.ccpc.ie/business/wp-content/uploads/sites/3/2017/03/CRD-Guidance_FINAL.pdf)

European Commission (2014) DG JUSTICE: Guidance document concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. Available from: [https://ec.europa.eu/info/sites/info/files/crd\\_guidance\\_en\\_0.pdf](https://ec.europa.eu/info/sites/info/files/crd_guidance_en_0.pdf)

Jelowicki, L. (2014) The EU Consumer Rights Directive 2014 explained. Practicology.com. Available from: <https://www.practicology.com/thinking/blog/eu-consumer-rights-directive-2014-explained>

Lindahl, F. (2013) The Consumer Rights Directive. Improved as a cross-border-only Regulation and toward a European Consumer Code, influenced by the Common Frame of Reference? Master's thesis in Commercial and Tax Law. Jönköping International Business School. Available from: <https://www.diva-portal.org/smash/get/diva2:623054/FULLTEXT01.pdf>

Schmon, C. (2016) Review of the Consumer Rights Directive. BEUC Comments. Available from: [http://www.beuc.eu/publications/beuc-x-2016-093\\_csc\\_beucs\\_comment\\_to\\_review\\_of\\_consumer\\_rights\\_directive.pdf](http://www.beuc.eu/publications/beuc-x-2016-093_csc_beucs_comment_to_review_of_consumer_rights_directive.pdf)

# **SECTION IV**

## **CYBERSECURITY**



## A. Introduction

There are many definitions for Cybersecurity; the most well-known being: “**Computer security**, also known as **cyber security** or **IT security**, is the protection of **computer** systems from the theft or damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide”[1].

Cybersecurity is a big and interesting research field in the Computer Science community. In this chapter we will mostly deal with Practical Computer Security, meaning the means in which Computer Security is applied in everyday settings. More specifically we will deal with the security of everyday processes in a business, even the smallest or newest ones.

Usually there are properties that affect computer systems. These properties could be related with hardware, software or even the network. Degrading that property may lead to consequences like theft, damage, disruption or misdirection of the data and business processes. Degrading this property may be deliberate, i.e. an attack, or accidental, i.e. fault. The most often situation is that of an attacker degrading the security of a computer system on purpose.

It sounds like a really terrifying and complicated issue, and usually it is. Nevertheless, people should not panic or act incorrectly. Placing all possible existing security controls in place simultaneously could be equally incorrect as with just doing nothing at all. Having too many security measures can raise several issues. It means additional work for your IT and security departments. Being an entrepreneur means that you probably don not have the privilege of having dedicated personnel for that, which could lead to spending too much money and time on the external partner that is providing you with the software or security measures. Furthermore, too many security measures, and black and white techniques; meaning techniques strictly designed and followed, will also mean too much work for the employees. If for example they have to go through numerous steps each time they want to connect to the invoice issuing software, then it will be difficult for them to actually work, and therefore time consuming. There is always the possibility that people will try to find another easier solution, a workaround. Such solutions would most probably be totally insecure and inappropriate. It is really important for businesses to be able to balance

security with performance. An important aspect that impacts performance in this respect is usability. Configuring security in software and making security-related decisions is a difficult task for many users. The manner in which security aspects are presented, in terms of their design and usability, makes it a complicated process, which users prefer to avoid and in most cases even ignore [21]. Reports identify human error as one of the most common causes of security configuration errors; mainly due to the non-user friendly design of security systems [21], [22]. Furthermore, using security systems that lack usability leads to users making mistakes that undermine the overall security [23].

All of the abovementioned can be translated to cost concerning a business. It is evident that there is a need for more flexible solutions that will provide customised methods for maintaining security according to the specific needs of each business or organisation. We can safely say that there exist several aspects to take into account when applying computer security.

Another point that is worth mentioning, is that security in a business regarding the digital data and processes shall also encompass the physical aspect and not only the technical one. Computer systems also comprise of the hardware devices that can get stolen or destroyed in some way. Some security measures could be taken to protect them, such as having them in proper facilities, always locking the room they are in, etc. Physical and technical (virtual) security can usually be combined in order to provide solutions in some situations. For example, if a laptop is stolen or a server is destroyed because of a fire, then if you had correctly backed up your data, you will be able to restore them and have the system up and running by using another hardware device. There could be losses, but they wouldn't be fatal for the business.

One extra step that each business can take is to spend some time educating its users (i.e. the employees, suppliers or anybody else using the system) on why and how to properly use the security measures and tools. That could save them work time from that time on, prevent users from trying to find a workaround and create security awareness in the working environment.

Cybersecurity is really important, not only because of the loss of data, time or money that a business can face if they encounter a security breach, but also because of the EU regulations regarding data protection that businesses will have to comply to,

since the GDPR became enforced on 25th of May 2018[19]. One could be in the difficult situation of not only facing business loss, but also having to deal with lawsuits, fines and courts.

In the next sections we present the following topics: Digital Security as a Technical Issue, Impact of Digital Security Breaches on Business Environment Processes, Cybersecurity Solutions and conclude with a Cybersecurity Checklist and a Terminology glossary.



## B. Digital Security as a Technical Problem

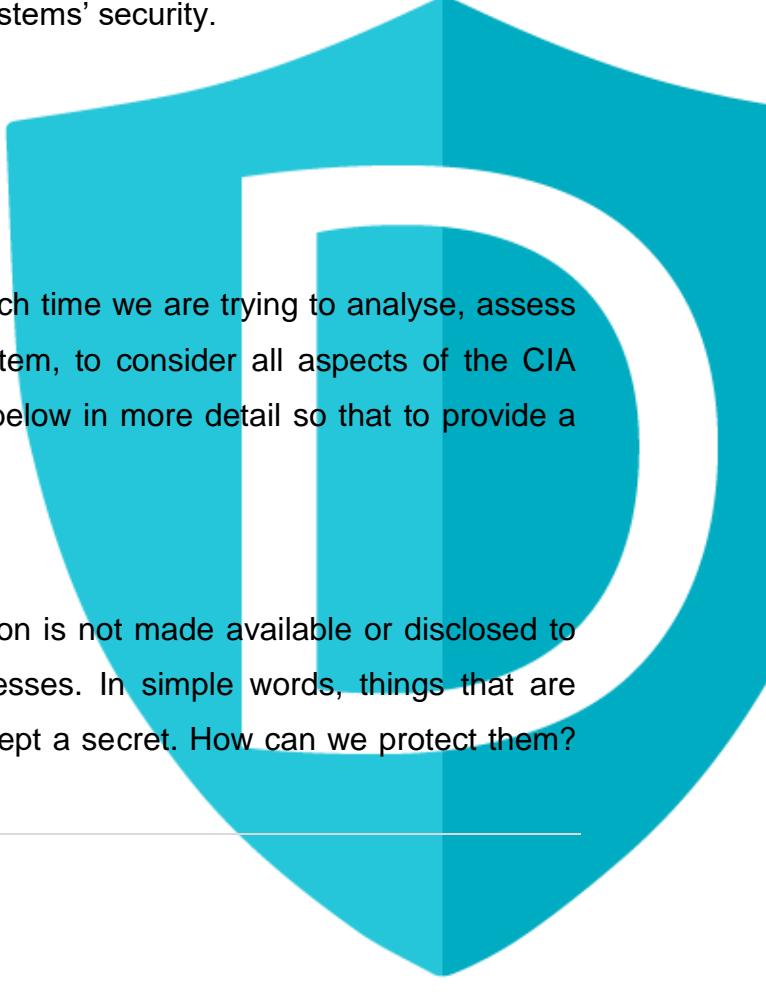
### I. Introduction

To begin with, we have to mention that Cybersecurity is not just a technical problem. What if the whole phone system goes down? It will not only affect the technical part of the business but also the processes such as the sales or purchases, the stock taking, the communication with the customers, etc.

As demonstrated above, technical aspects of Cybersecurity can directly affect the whole business. That is the practical side of Cybersecurity. As such, acquiring more knowledge regarding its technical aspects is fundamental for facing and handling a crisis of that kind.

Different applications have different security requirements, which can be grouped by the following principles: Confidentiality, Integrity, Availability, Authentication, Non-Reputation, Accounting, Privacy, and more. The three most important principles, referred to as the CIA Triad, are **Confidentiality**, **Integrity** and **Availability**. Businesses' computer systems must be protected on all of the three levels at all times. Degrading any one of them means larger risk in your systems' security.

### II. The CIA principles triad



As explained above, it is really important each time we are trying to analyse, assess or implement security in any computer system, to consider all aspects of the CIA principles triad. Each of them is described below in more detail so that to provide a better understanding.

#### ***Confidentiality***

Confidentiality principle states that information is not made available or disclosed to unauthorized individuals, systems, or processes. In simple words, things that are supposed to be kept as a secret, must be kept a secret. How can we protect them?

How important is to protect them? Can those secrets be used against the associated individual? As an example, imagine someone stealing your online shop clients' credit card information. Moreover, there are many other data that usually must be kept secret including intellectual property, financial information, government secrets, student data and more. Confidentiality is very important as laws and regulations are based on it. The damage caused by loss of confidentiality, for example by a data breach, can be severe. This is the most sought-after principle of the CIA triad and the one people are usually most familiar with. There are everyday examples on how we use and protect Confidentiality. One example is the usage of encrypted channels for communications across the internet, as in the situation where we have the login credentials go through "https" instead of "http" to maintain a completely encrypted communication between the client and the server, in order to keep them confidential. A website owner needs to acquire the certificate for "https" and use it in order to take advantage of this safe communication. Encryption is already implemented by the https protocol. As stated on Google's announcement: Beginning in July 2018 with the release of Chrome 68, Chrome will mark all "http" sites as "not secure". Read more on the official Google announcement in [8].

Another example is the usage of a Virtual Private Network - VPN network to connect if we are travelling instead of just using any untrusted available wi-fi that may be unsafe. A VPN is a "tunneled" secured network through a Wide Area Network (WAN), such as the Internet, that enables secure communication between its endpoints. The person connected to the VPN is in reality securely connected to the (secured) Local Area Network (LAN) of his/her business while away, meaning that he/she does not have to be actually located to the physical location of the business's LAN in order to be secured [2]. VPN offers encrypted communication between client and server and it is owned by an organization in order to control and monitor the traffic that passes through it. In case of an attack, the organization will be able to find through the VPN Network the requests that are passed to or from it, which usually reveals who the attacker is.

Another example is the usage of encryption software to encrypt volumes of data. Such software is BitLocker that is a Windows' technology and FileVault that is the Mac's solution. Encryption could actually be seen as the technical implementation of

Confidentiality. Having really important data encrypted can make them remain secret even in the case that they get stolen, since the files would be unreadable to anyone who does not possess the appropriate decryption key.

There are several encryption algorithms and methods that can be used to encrypt and protect your data. AES is the most well-known and recent one. So how can someone use this knowledge?

As illustrated in Figure 1 below, the steps are as follows:

First thing to do is to select a cryptographic algorithm to apply, that comprise the Crypto System. The cryptographic algorithm is public and known to anybody without affecting the security of the encryption.

Second, select a key to encrypt that will make the data unreadable. The key should definitely be kept as a secret as opposed to the cryptographic algorithm.

Now as a next step, having the key and the information that you want to encrypt, you can then provide them to the Crypto System, that will produce the encrypted data called the Cipher Text.

You are now able to send or store the Cipher Text. Even in public, nobody without the decryption key can access it.

If you want to use these data, decrypt them using the matching key.



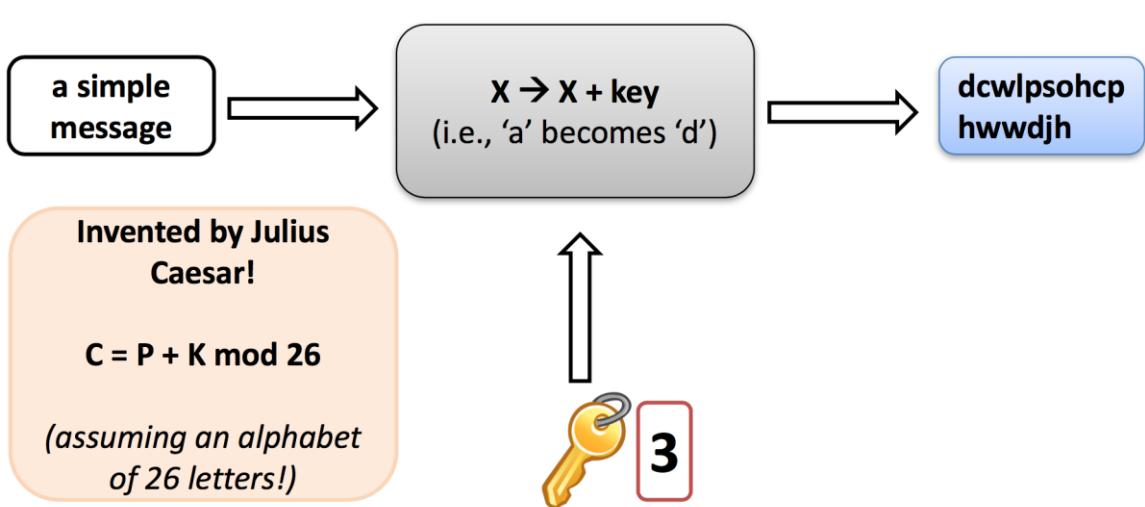
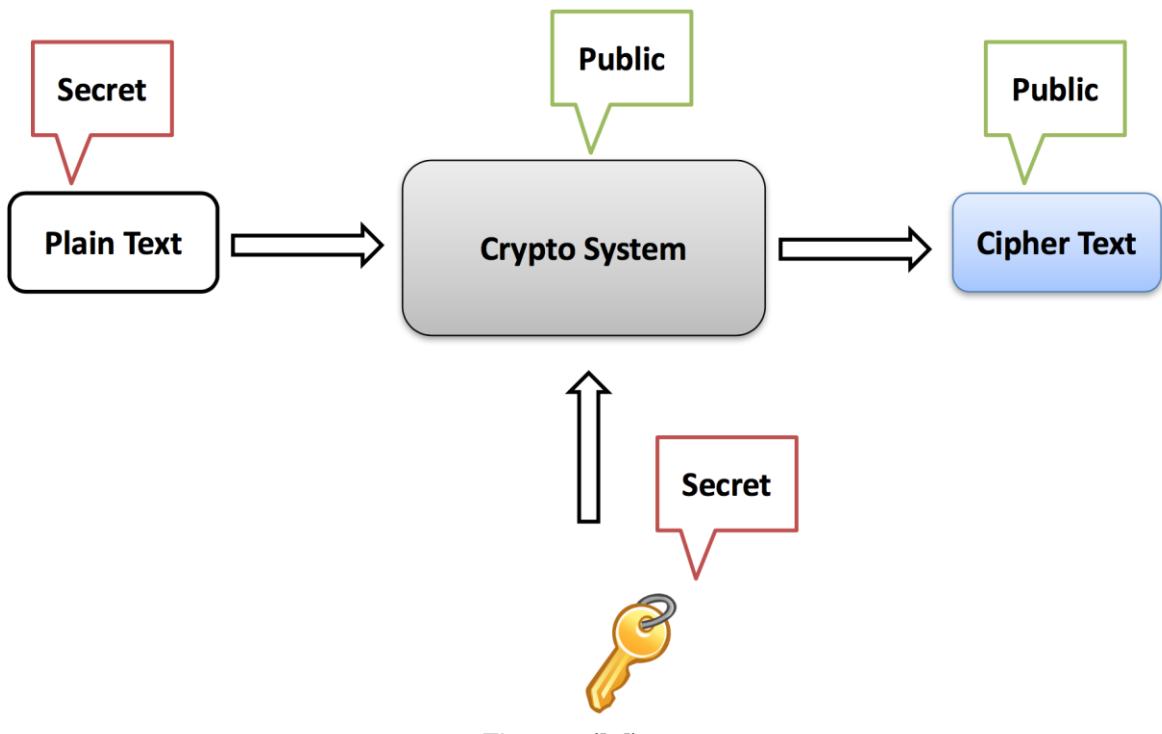


Figure 2([6])

Let's assume we have the following text we want to encrypt: "a simple message". The text is now meaningful, and everyone understands what it says. If someone obtains unauthorised access to the server to view or acquire data from it, he/she will see the text "a simple message". We chose to use Caesar Cipher as our

cryptographic algorithm. This algorithm basically shifts the letters in cycle having an alphabet. We also decided that our key is the number “3”. Please note that, while keys need to be complex, this is simple just to be used as an example. In order to be in cycle, every character in the text “a simple message” will be moved by +3 letters. At the beginning, we divide the key ( $k=3$ ) by 26 (the letters in the English alphabet). Then we move the letter according to the remainder of the division and so on. As a result, we will have the message as “dcwlpsohcp hwwdjh”. This is definitely not readable! We can store it somewhere or send it to another end. If we want to read this message using our key, we are simply applying the process described above in reverse. Meaning that we subtract our key from each character etc. [Figure 2]

Let's see now how we measure a strong encryption key by providing an example. Brute-force attacks basically mean trying all possible combinations on achieving something (eg. break a password or find an encryption key with a range of possible combinations). A 4-bit long encryption key has  $2^4$  possible combinations and equals to 16 key tries to break the encryption. This is really easy to break instead of a 32-bit long encryption key, which has  $2^{32}$  possible combinations equals to 4 294 967 296 key tries to break the encryption. Imagine using an even bigger key of 64-bits long! It will take an unbelievable amount of time making it somehow impossible to break the encryption. Now consider our example in Figure 2 where the key used needs just 2 bits to be represented: with 2 bits we can get a number from 0 to 3, i.e. only  $2^2=4$  combinations. An attacker applying a brute-force attack will need in the worst case only 4 attempts to find our key.

By now, it should be totally clear why we need to comply with the principle of Confidentiality. It can protect us from people intentionally or accidentally leaking our secret or sensitive data, and provide access only to authorized individuals.

### ***Integrity***

Integrity principle states that data or information has not been changed, destroyed, destracted or in any way modified or lost in an unauthorized or accidental manner.

In simple words, information shall be kept accurate and complete, comprising “the truth” coming from the source. To discuss some everyday examples of how we use and protect Integrity, we can begin by saying that Integrity allows us to verify data

traversing the network and specifically check packets for errors using the Cyclical Redundancy Check (CRC) method. CRC is a hash function that detects accidental changes to raw computer data commonly used in digital telecommunications networks [20]. If there are errors, then information is resent and checked again and so on. Another example is that of Digital Signatures; a cryptographic algorithm ensuring that the person that actually sent the information was the one meant to send it. One further example is Cryptographic Hashing Algorithms such as MD5 or SHA1. They compare the file actually downloaded, for example a software, to the originally offered download by creating a fixed length hash value, the digest. Even a small change in the file will bring a huge change in the output (digest).

One example is that of phpMyAdmin attacks. The attacker may manage to replace some of the binary files of this very commonly used software, preventing hashing and checksum checks in succeeding.

Integrity and accuracy are really important and needed. If we can't verify that a message we received is "good", then what is the purpose of receiving it? Imagine watching a video or a movie with distorted information. Can you later use this knowledge acquired as correct or have you missed some important information?

### **Availability**

Availability principle states that an information system or a system resource i.e. information remains accessible and usable upon demand by an authorized system entity, for example a user, according to performance specifications for the system. A system is available if it provides services according to its design either upon users' request or in a continuous manner.

In simple words, systems must be available and functioning and data able to be accessed whenever we need them to be. Consider the example of a PC going down while a user is doing some important work on it or that of a catastrophic virus wiping out a whole computer system. It might even be a life and death situation, in the case for example of patient medical records not being accessible in a case of emergency.

What about in the case where devices are completely destroyed and thus, not only services, but data get lost as well? Do you have them backed up to restore them as soon as possible, thus restoring that way availability as well? What about the case where the backed-up data were stored at the same physical location as the original, and all of them have been destroyed during a fire? Do you need to have more than one back up in different locations, or devices, or data centers?

Some ways that we can use to ensure better and more suitable backup to enhance data availability include: incorporating *RAID levels* that group data into levels in data centers servers depending on how much we need that data to be available, *server clustering* meaning to have different data centers but all of them providing data to the same website with the user having no clue about that, and using *load balancers* to have the data of the users going to available servers for example in the case one is down.

An example of attack on a computer system that leads to failure of Availability is the Denial of Service attack. A denial-of-service attack (DoS attack) is a cyber-attack in which the attacker seeks to make a machine or network unavailable, so that no user can use it normally. It may interrupt user's experience through a service. So, the service is basically "down" and cannot be used regularly by the clients.

DoS Attack is accomplished by overloading the target machine or network with a huge number of requests in an attempt to overload these systems and fully or partially prevent some requests from being completed.

In contrast, during the distributed denial-of-service attack (DDoS attack), the incoming traffic overloading the target system originates from many different sources. This makes the attack impossible to stop because to achieve this we will need to block every attacker targeting our system.

A DoS or DDoS attack is similar to a crowd trying to access the entry door or gate to a shop or business, and thus not allowing legitimate parties enter. This could disrupt normal operations of the shop or business. Attackers that use the DoS method, often target sites or services hosted on high-profile web servers such as banks or credit card payment gateways.

Below you can graphically view an applied example of how the three principles that we discussed are affecting the communication between the system and a user and how important they are for the security of this communication.

Let's assume that the user wants to communicate through the internet with a system or service. It could be your client communicating with your online shop service. The user must have the service offered without any issues that could cause the service to not act properly (availability). The user wants to secretly send messages to the system/service without any unwanted eyes reading their messages (confidentiality). Along with that, no one should have the ability to change those messages in any way and thus alter the original data that the user sends or receives (integrity). [Figure 3]

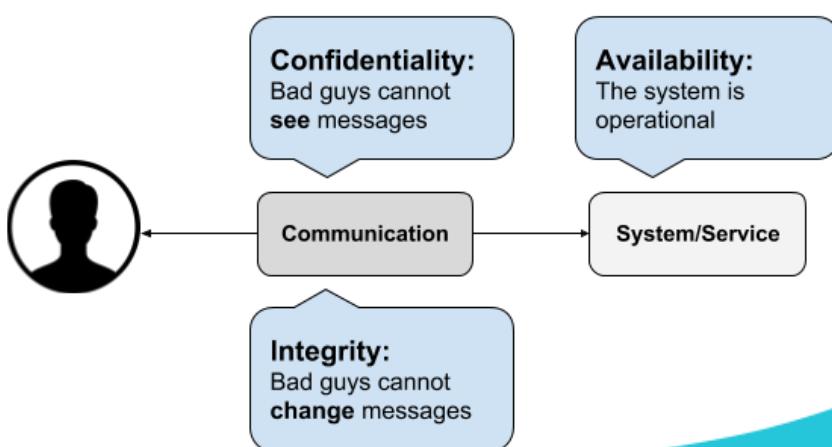


Figure 3, based on [6]

### III. Risk

Risk in your system can be measured by the probability of loss of one of the three CIA security principles analysed above. Don't think that risk is only referring to big threats or attacks. Risk can be everywhere even in the simplest thing.

A more detailed discussion about risk is provided in Chapter V.

## IV. Common attacks review

### ***Malware***

The term malware is a conjunction of the words “malicious software”. In simple words, malware is any piece of software intent on doing harm to data, devices or to people. Such software is designed and developed with the purpose of destroying data, affecting the computer’s performance, causing a crash or spying on private information.

Historically, malware was disseminated to users via email attachments. The email directly received by the user was asking him to click on the attachment. The click was activating and executing the malware and ultimately doing the intended harm [7].

Each kind of malware acts in a different way in order to infect and harm computers and data, thus each of them requires a different malware removal method. The Best practice that you can follow is to use antivirus software that includes malware removing tools. Also, don’t forget to avoid suspicious emails or links [17].

Different well-known types of malware are Viruses, Trojans, Spyware, Worms, Ransomware, Adware and BotNets. In short:

A ***Virus***, as suggested by its name, attaches itself to clean files, copies itself and propagates by infecting other clean files and computer systems. This propagation can be uncontrollable. The damage of such an infection can be severe or even unreparable e.g. damage in the system’s core functionality, destruction and deletion of files etc. A Virus usually has the form of an executable file and it gets activated when you run it (by clicking on it) [7], [17].

A ***Trojan*** disguises itself as legitimate software or is included in one such that has been tampered. As the name suggests, it acts discretely and creates backdoors in the system’s security to actually let other malware in [17].

***Spyware*** is a malware designed to spy on your information. It is almost always bundled with free software and quite often is the price you have to pay for using that software. It can be a minor annoyance e.g. having advertisements pop-up, change of settings without your consent or action, or it can have a serious impact on the

computer system e.g. dramatically slowing down the system's performance. It can also be the case that the Spyware would hide in the background and take notes on what you do online, including your passwords, credit card numbers, surfing habits, personal or financial information and more. Furthermore, it could take remote control of the computer to access files and data, to install software or to use the computer to help spread viruses [7], [17].

**Worms:** A worm is a type of virus but with the basic difference that it has the ability to spread automatically without human initiation (while a typical virus spreads through human activity e.g. by running an executable file). A worm can spread from computer to computer, by exploiting software and hardware vulnerabilities by using each consecutive infected machine to infect more [17], [18].

**Ransomware:** A ransomware is a type of a malicious software that gains unauthorized access to your computer systems and encrypts your files. This way it can hold them as "hostages" along with the whole system or device, blocking you from accessing them until you pay the ransom asked in exchange for the decryption key [4]. Ransomware is explained in more detail in following subtopics.

**Adware:** Adware is not directly threatening a computer system as other malware do, as it is an advertising software. The problem is that it can undermine your security to serve its purposes, thus giving other malware a way into your system [17].

**BotNet Attack:** Attackers usually try to compromise servers containing valuable data about a business or its users. A way to harm or use a compromised server is by controlling several ordinary hosts (e.g. a computer) as bots. Those bots can comprise a BotNet (like an army of compromised machines, see Figure 4) [6] that can be used in various ways of attacking other hosts, keeping the anonymity of the attacker.

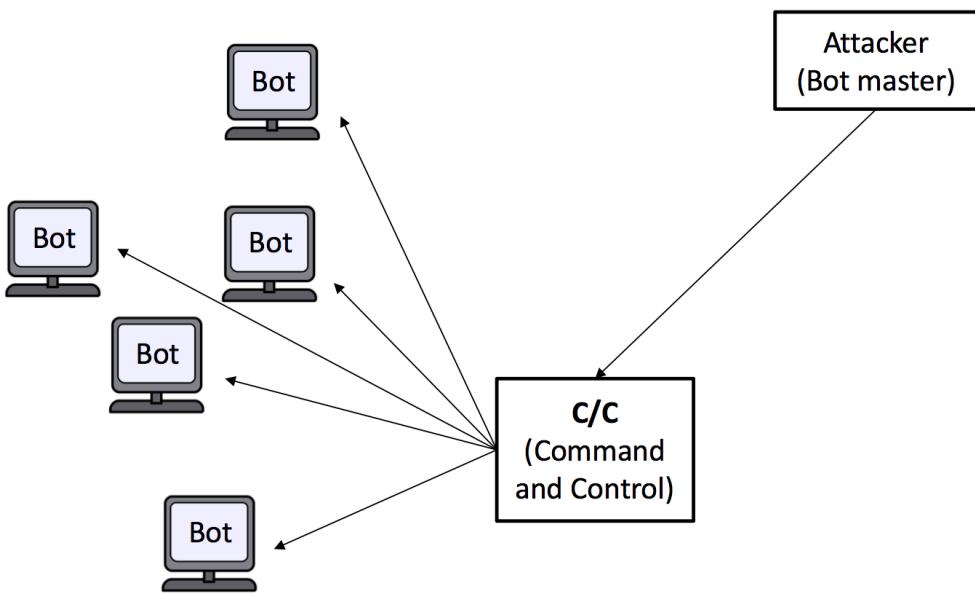


Figure 4

A BotNet is basically a large collection of compromised hosts that can be controlled by an attacker called Bot Master. These networks are often used via rent for all sorts of malicious activities. For example, someone could find a Bot Master and ask from him to use his BotNet to click fraud on a link in order to make more money or fake traffic, send SPAM emails to a range of emails, gain fake Facebook/Twitter likes or retweets. One of the most ideal uses of an attacker renting a BotNet from a Bot Master is the Distributed Denial of Service (DDoS) attacks to target host(s).

Bot Master controls the BotNet through a hidden command and control channel (BotNet C/C). The bots are periodically checking this channel to receive new commands. Commands often come from somewhere public, see Figure 5 [6]. For example, a twitter account made just for this kind of attacks. The attacker tweets an encrypted command so that no one understands what the commands is. BotNet C/C can understand the command by using the key of the attacker, decrypt it and execute.

Twitter

Home Profile Find People Settings Help Sign out

o\_O upd4t3

Follow

aHR0cDovL2JpdC5seS8xN2EzdFMç  
about 2 hours ago from web

aHR0cDovL2JpdC5seS9MT2ZSTyBodHRwOi8vYml0Lmx5L0ltZ2  
about 2 hours ago from web

aHR0cDovL2JpdC5seS8xN2w0RmEgaHR0cDovL2JpdC5seS8xN  
about 4 hours ago from web

aHR0cDovL2JpdC5seS9wbVN1YyBodHRwOi8vYml0Lmx5LzE3b  
about 4 hours ago from web

aHR0cDovL2JpdC5seS9HaHVvdSBodHRwOi8vYml0Lmx5L1FqC  
about 5 hours ago from web

aHR0cDovL2JpdC5seS9RakFaWQ==  
about 5 hours ago from web

aHR0cDovL2JpdC5seS83UGFEOQ==  
about 5 hours ago from web

aHR0cDovL2JpdC5seS8zUndBTiBodHRwOi8vYml0Lmx5LzJwU0  
about 5 hours ago from web

Name upd4t3  
20 following 7 followers  
Tweets 25  
Favorites  
Actions block upd4t3  
Following  
RSS feed of upd4t3's tweets

Figure 5

### Let's see a few famous examples of the above:

In 2000, “ILOVEYOU” virus, was the most damaging malware event of all time. The virus came in an email with a subject line that said “I love you”. “ILOVEYOU” overwrote system files and personal files and spread itself over and over and over again [24].

“Storm Worm” was a Trojan horse that infected computers, sometimes turning them into zombies or bots to continue the spread of the virus and to send a huge amount of spam mail. Devices got infected when people were opening an email headed “230 dead as storm batters Europe” and clicking on the link. By July 2007, Storm Worm was picked up in more than 200 million emails[24].

A very famous example of Ransomware is CryptoLocker, Released in September 2013, spread through email attachments and encrypted the user's files so that they couldn't access them[24].

### ***Web-based Attacks***

Web-based attacks are those that make use of web-enabled systems and services, including: browsers (along with their extensions), websites (including CMS - Content Management Systems), and the IT-components of web services and web applications.

There are different types of those attacks, such as:

- web browser exploits (or their extensions),
- web servers and web services exploits,
- drive-by attacks,
- water-holing attacks,
- redirection and man-in-the-browser-attacks.

Web browser exploits are forms of malicious code that use vulnerability in an operating system or an installed software, with the intention to breach browser security and to change users' browser settings, without their actual knowledge [32].

Web servers and web services exploits are piece of software or a chunk of data, which takes advantage of a bug or vulnerability of a web server or web services, to cause unintended or unanticipated behaviour. Such behaviour can allow attackers for example to remotely take control of affected web server or web service, over the Internet and allows them to remotely execute malicious code.

Drive-by attacks, concern the unintended download of computer software from the Internet and mean two things:

- downloads which the user has started, but without understanding the consequences, for example a download which installed an unknown executable program, ActiveX component or Java applet, automatically,

- downloads that happened without the user's knowledge, such downloads can be initiated by simply visiting a website or viewing an html e-mail message, with planted malicious script into HTTP or PHP code [33].

Water-holing attacks are attacks in which the attacker guesses or observes which websites are often visited by a victim or a particular group (meaning organization, industry or region) and infects one or more of those websites with malware. A watering hole is a kind of computer attack strategy, in which the victim is a particular group of users and this attack has the potential to infect the members of the targeted victim group through specific configurations for the malware, to be able to select the targeted users from the infected users [34]

Redirection visitors of a legitimate website to another website is possible with inserting a malicious code inside a configuration file of a web server. Then the attacker wants users to enter sensitive information into a malicious website while seemingly navigating within a trusted website. Man-in-the-browser-attacks are designed to intercept data as it passes over a secure communication between a user and an online application [35].

### ***Web application Attacks***

Web application attacks are directed against available web applications, web services and also mobile apps. Such attacks try to abuse APIs that are incorporated in web applications. Web application attacks are usually targeted at well-known resources and open-source or public-source based projects, such as Joomla and Wordpress plugins, Magento sites, etc.

Such types of web application attacks can be listed:

- SQL Injection (SQLi) attacks,
- Local File Inclusion (LFI),
- Remote File inclusion (RFI),
- Cross-site Scripting (XSS),
- PHP injection (PHPi) or PHP Object Injection [36].

SQL Injection (SQLi) attack is a code injection technique. It is used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution. SQL Injection is one of the most critical vulnerabilities. An attack based on a SQL Injection vulnerability, permits to dump database contents, such as: names, credit card numbers and any other sort of confidential and sensitive commercial data [37].

Local File Inclusion (LFI) mans an inclusion attack in which the attacker can trick the web application in including files on the web server by exploiting functionality that dynamically include local files or scripts. The consequence of such an attack include: Directory Traversal and Information Disclosure or even Remote Code Execution. Local File Inclusion is very similar to Remote File Inclusion (RFI).

In RFI the attacker, comparing to LFI, can not only include local files, but also remote files [38].

Cross-site Scripting (XSS) is a kind of client-side code injection attack, where the attacker can execute malicious scripts, into a legitimate website or web application [39].

PHP injection (PHPi) or PHP Object Injection is an application level vulnerability, which actually allows the attacker to make different kinds of malicious attacks, such as: SQL Injection, Application Denial of Service, Code Injection and Path Traversal based on the context [40].

### ***Denial of Service Attack***

Denial of service (DoS) attack is an attack with the intent to shut down a machine or a network, making it inaccessible to users. Denial of service attacks are usually accomplished by directing big traffic or sending information that causes a crash. In both case, the Denial of service attack denies employees, members or account holders, so actual legitimate users, of the service or resource. Banks, commerce, media companies or government and trade organizations and other high-profile organizations are usually the victims of Denial of service attacks. Denial of service attacks usually do not result in theft or loss of information or other assets but take much time and money to handle. A different type of DoS attack is the Distributed Denial of Service (DDoS) attack. A Distributed Denial of Service attack happens

when multiple systems carry out a synchronized DoS attack on a single target. The difference is that the target is attacked from many locations at once [41].

### ***Spam***

Spam is as old as the Internet itself. But still it remains the main mean of malware delivery, using malicious attachments and malicious links. Spam is over 85% of all sent e-mails and spam accounts are more than 50% of volume of e-mail addresses. Spam is sent by large botnets or virus infected computers and can also be a channel to advertise healthcare products or erotic/dating services. It is important the users ask themselves before opening an e-mail, if they know the sender, if the attachment format and content is correct, if they recognize the subject of the e-mail [42].

### ***Phishing***

Phishing primarily uses social engineering techniques to attack end users. Those techniques are used to deceive users and exploits weaknesses in web security. Phishing attacks usually start with a malicious e-mail that the users receive, in which he or she is convinced to visit a fraudulent website, which attempts to obtain sensitive information such as usernames, passwords and credit card details, often for malicious reasons. A Phishing email for example could state that it's from your bank officer and asking you to kindly provide your net banking login credential to help you resolve the issue that they recognised that you have, or red cross volunteers asking for your credit card number in order to accept your donation for people in need, and so on. You will have to be really careful, reason logically about everything and have in mind that organisations would never ask for your credentials through email. Not everything is trustful. There is a big possibility that it may be an attacker trying to steal valuable information from you.

Phishing is also becoming more and more sophisticated and targeted, which makes its detection increasingly difficult. Instant messaging, not only e-mails, is also often used.

Phishing could be also appeared through a fake website that looks very similar to other popular ones. What is important those fraudulent websites usually look identical to legitimate websites and the only difference is the URL of the website. For example, somehow or someone can redirect you to a website called

[www.bankofvwest.com](http://www.bankofvwest.com) instead of [www.bankofwest.com](http://www.bankofwest.com). They look alike but the first one is a fake controlled website from an attacker in order to get your personal info, bank accounts, credit cards etc. The latter example could be avoided with the right use of certificates that will be described further in a later section. In general, phishing campaigns have increased both in volume and sophistication. Phishing is usually used as the first step in cyber-attacks. Because of this phishing is linked to most of the cyber threats, such as: botnets, malware, web-based attacks, exploit kits, cyber-espionage, etc. [43]

### ***Insider Threat***

Insider threat, according to its definition, refers to a threat that an insider user will use his or her authorized access, either intentionally or unintentionally, to harm the organisation's security. Because of this insider threats are a major risk to various institutions and organisations, regardless of their location, size or sector. It is always difficult for most organisations to distinguish them from a nonthreatening activity. Insider incidents can be deliberate or inadvertent. What is important to mention however is that losses due to an insider threat are largely unknown. But it is the privileged users, including managers with access to sensitive information, who pose the biggest threats to the organization [44].

### ***Identity Theft***

Identity theft is a special case of data breach. It is an attack aiming to obtain confidential information that can be used to identify a person or even a computer system. This information then can be further used to impersonate the owner of the identity. Attackers aim to obtain such information as: identifiable names, addresses, contact data, credentials, financial data, health data, logs, etc. Once the attacker possesses personal information, they can drain out the victim's bank account, run up charges on victim's credit cards, open new utility accounts or even get medical treatment on victim's health insurance. A thief might even give the victim's name to the police during an arrest. According to the Federal Trade Commission, an independent agency of the United States government, identity theft falls into six major categories: employment-related or tax-related fraud (using someone else's personal information to gain employment or to file an income tax return), credit card

fraud (using someone else's credit card or credit card number to make fraudulent purchases), phone or utilities fraud (using another person's personal information to open a mobile phone or utility account), bank fraud (using someone else's personal information to take over an existing financial account or to open a new account in someone else's name), loan or lease fraud (using someone else's information to obtain a loan or lease), government documents or benefits fraud (using stolen personal information to obtain government benefits) [45].

### ***Information Leakage***

Information leakage is a major cyber-security threat. Information leakage means various types of information leaks, starting from personal data collected by Internet giants and online services, even to business data stored in companies' IT infrastructures [46].

### ***Cyber-espionage***

Cyber-espionage means stealing secrets and information stored in digital formats or on computers and IT networks, without the permission and knowledge of the holder of the information, from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage. Cyber-espionage involves typically the use of such secrets and information or even control of individual computers/whole networks, for a strategic advantage or for psychological, political activities and sabotage. Recently cyber-espionage involves also an analysis of public activity on social networking sites, including Facebook and Twitter [47]. In most cases the users or organizations whose digital security has become compromised aren't even aware of it. But what are the best protection forms from technical risks in regard to digital security, such as: malware, web-based attacks, web application attacks, phishing, spam, denial of service, ransomware, botnets, insider threat, physical manipulation, data breaches, identity theft, information leakage, exploit kits, cyber-espionage? Simple, common-sense precautions when using the Internet and other new technologies, can prevent from exposure to the above mentioned technical risks. Computer's operating system should be updated as early as possible (automatic updates should be considered), as hackers often utilize known flaws in operating system security for their aims. Regular updates are also of high importance

to different applications on computers, smartphones, tablet or even Internet of Things devices, as once weakness are found and announced by software companies, hackers start to create programs to exploit those weaknesses. Web applications, web services, websites (including CMS - Content Management Systems), should also be regularly updated. Browsers and plugins should also be updated to the latest version. Users should not download attachments or click on links from e-mail messages that are suspicious and especially coming from e-mail addresses they don't recognize. Firewall software and Internet security suite, anti-virus software should be used and updated regularly, especially when browsing the Internet. Suspicious websites should not be visited. Passwords used should not be simple and changing passwords often (every 4 weeks) is also suggested. Regularly back-up your data and store back-ups in a safe location. IT administrators should ensure that all systems in the network are patched and updated. Individuals should be careful of what you share on social media, they should not list too many details on their profiles [48].

## V. More potential problems for a business

Different threats are continuously rising, trying to fraud people by using new and admittedly creative ways. Such are:

- Scam telephone calls, which are similar to phishing emails. People very convincingly say that they will be needing some information from you regarding a fake problem. For example, they could say that they are calling from Microsoft and they have discovered that you have a virus on your system. So, in order to be able to help you, they will be needing your login credentials and other information.
- The physical presence of unauthorised people in your data center room, or in front of your computer or laptop. Perhaps it could be somebody who broke into your premises to steal data or even someone pretending to be a customer but actually staring at the data presented on your screen while you browse your system trying to answer his questions about prices and stock.

- Ransomware is a really big threat to all sized companies, from the smallest entrepreneur to the biggest enterprise. It is an attack where the threat agent gets access to a computer, encrypts all data in such a way that it cannot be used any more and then asks for ransom in order to decrypt them. A detailed example will be given in the next two sections.
- Last but not least, more intelligent and more flexible viruses and other malware are appearing all the time as a threat. Investing in a good antivirus software that constantly updates its virus database would be a very good and effective solution to that.



## C. Impact of Digital Security Breaches on Business Environment Processes

### I. Impact

We have already described cases above in which having a technical failure in a business computer system because of lack of security could lead to disruption of business processes. One way or another if the system or a part of it collapses, that means cost for the business. Cost doesn't always mean money, it can mean loss of time or effort, loss of future or casual customers, loss of valuable data, or even facing a lawsuit.

From the simplest thing such as having the internet down for a few minutes, to the most serious cases such as your client's information being stolen, bad things can happen.

Missing a deadline, not being able to issue invoices or receipts, not being able to complete a transaction or a sale, failure to deliver an order on time, having sensitive data exposed or used, losing all of your accounting data, having your admin credentials stolen are only few of the situations that entrepreneurs may find themselves in due to the inadequate security configuration of their system.

What if someone steals your credentials, logs in to your online shop and takes it under his control? If you don't have a back-up plan you may even just lose your whole business.

As previously mentioned, a *ransomware* attack is a serious situation. Let's use this example as a **case study** in this chapter.

### II. Case Study: Ransomware

A **ransomware** is a type of a malicious software that gains access to your computer systems and by encrypting your files can hold them along with the whole system or device as "hostages", blocking you from accessing them until you pay the ransom asked in exchange for the decryption key. As we have explained in the previous chapter, encrypted data are unreadable unless you possess the key [4]. Of course,

even if the ransom is paid, no one can guarantee that the decryption key will be eventually provided. Remember that you are dealing with criminals that only care about your money and not about your data. If they ask for your banking details or credit card data and you provide them with those, they maybe try to maximise their profit by using that info even after they send the decryption key (if they do). Or they may send you an “unlock” file that may infect your PC with yet more malware [28].

You can get ransomware from an email attachment, a malicious downloaded file, a hacked website or a seemingly innocent but actually malicious advertisement. Using cracked software, P2P Networks, or a ransomware-infected USB could potentially infect your device [29]. Once you are infected with Ransomware you will notice that your files, images and data have been encrypted and you are unable to open them. You could also get a popup screen asking to pay the ransom, followed by a threat.

Ransomware attacks have been around for decades but are holding steady as one of the most significant threats that businesses and individuals face today. As previous ransomware software is getting prevented, their variety is growing increasingly advanced in spreading capabilities, evading detection, in encrypting files and forcing users into paying ransoms. Each new such software is more sophisticated, more challenging to prevent and more damaging to the victim.

A historical fact is that the first ransomware attack that we know of happened in 1989 and the target was the healthcare industry, which is actually still one of the top targets for such attacks. Some advanced cybercriminals are making ransomware a serious money-making business by offering ransomware-as-a-service programs. Some of the most well-known ransomware are CryptoLocker, CryptoWall, Locky and TeslaCrypt. CryptoWall alone has generated more than \$320 million in revenue.

Ransomware average demands today are around \$500. Usually a deadline is given to the victim to pay the ransoms, stating that if the deadline passes the demand would double or the files will become permanently unavailable or destroyed or even exposed publicly.

Therefore, it is obvious that a Ransomware attack could have a significant and really negative impact on a business, whether it is owned by an entrepreneur or it is a huge well established enterprise company. Availability becomes a huge issue, and if you

are not prepared and ready to recover then it will be either loss of data or loss of money, with all the consequences coming along with them.

If you need more info you can read details about the top 10 worst ransomware attacks of 2017 in [9].

At the end of the next chapter, we will discuss actions that can be taken in order to resolve such an attack, caused by Ransomware.



## D. Cybersecurity Solutions

### I. Security Frameworks

It can be a frustrating and confusing to implement security on your computer systems. To assist in this task, you can make use of guides such as Security Frameworks and standards, which explain how to comply with security and also point out what should be avoided. By following these guides, you can enhance and validate your security. The more general frameworks can be applied to almost any business and one is able to choose which guidelines to follow from it. Examples of such frameworks include the NIST Frameworks [25], the ISO Frameworks [26] and the CIS Framework [27].

When deciding on which framework to choose, consider one that is relatively easy to follow and seems more suitable for you. Once you have chosen the framework, decide which controls best suit your business. Depending on your business's processes and needs it may not be necessary to comply with everything or implement all measures right from the start. This leads to you creating your own security policy framework to follow and elaborate.

### II. Other security solution measures

In the previous sections numerous measures were referred mostly as examples. To summarise, some measures that can provide solutions to Cybersecurity threads are the following:

- Proper and regular backup of all data;
- Installation of antivirus and firewall software with the proper specifications for each device. Please keep in mind that sometimes is worth purchasing this kind of software rather than using free or trial versions of them;
- Regular updating of your systems;
- Compliance to a security framework or part of it;
- Choosing strong passwords and protecting them by not sharing them with anyone and not letting them be exposed;
- Acquiring an https certificate for your website;

- Prevention of unauthorised individuals having physical access to your premises or devices;
- Only using software from trusted sources, that is validated and verified and embeds all necessary technical security measures.

There exist numerous online tools that you can use, either to assess your security or to identify whether your security has been breached.

- Security assessment tools can be useful for checking how well you have implemented security measures in your business. One example is the Microsoft Security Assessment Tool that can be found and downloaded in [10]
- Tools that will help you learn of any compromises of your email accounts. Some of them also highlight the severity of the risks of online attacks on today's internet. One example is the "Have I been pwned?" tool that can be found in [11]. All the data on this tool comes from publicly leaked "breaches" or in other words, personal account data that has been illegally accessed then released into the public domain. "Have I been pwned?" aggregates it and makes it readily searchable.

### III. Case Study Part II

Revisiting the Case Study about Ransomware, we can analyse the steps that are needed to resolve such an issue.

First of all, you must understand that by the time you realise that you are under attack by such software, your files (all or some of them) will already be decrypted. So how shall one react?

The **first step** is to **stop the attack**. In order to do that you should cut off access of the infected device to the network. If it is the case that you have a centralized file directory, meaning a server with all the documents located there, and users connected to it from separate devices, you should cut off user "*write*" access to this server for all users. You must do this because, as ransomware operates via a user infection, you must stop the infected user from accessing further any data on the server. A way to do this is by making the server "*Read-only*" so no user could write to it. Of course, this will have the negative impact of disabling the write access for all the

“innocent” users as well. It is really important not to turn off the server. It is needed to be up and running with all of the recent logs available.

You now need to find the infected user so that to maintain server access restrictions only for him/her and permit access to the other users. You can find who this person is by checking who has had permissions to the attacked files, and who has accessed them before the attack. The infected user should be instructed to immediately unplug the ethernet cable to disconnect from the network (or disconnect from the wi-fi network), thus the attack would stop. Note that the user should not shutdown the computer because there might be vital information about the attack within the computer’s memory that will be deleted when cutting off the power.

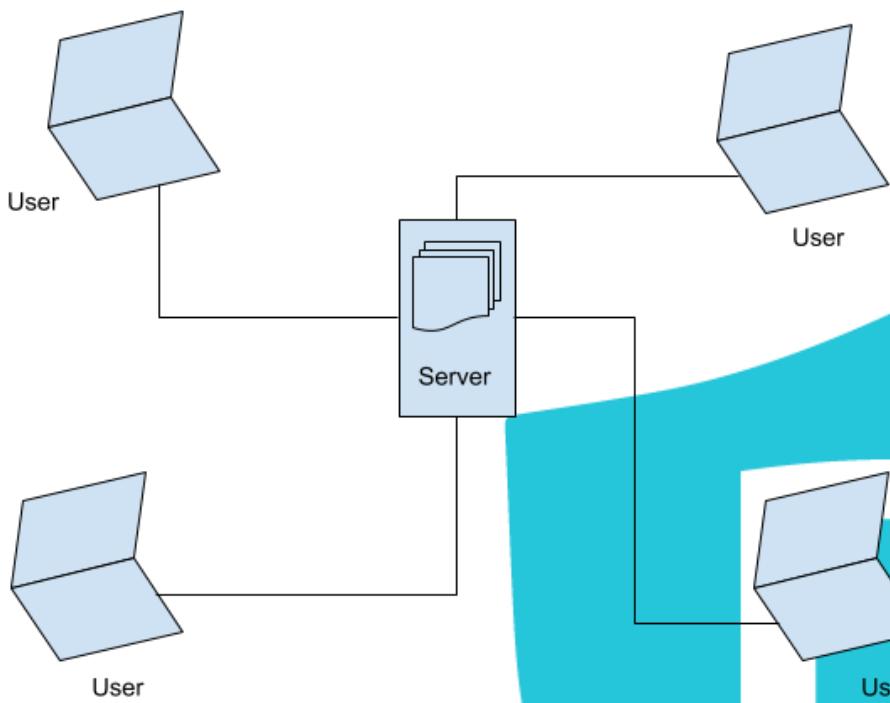


Figure 8 - Centralized File Directory

If you are a single device user with the files located on your device, remove your device from the network but do not shut it down for the same reasons explained above.

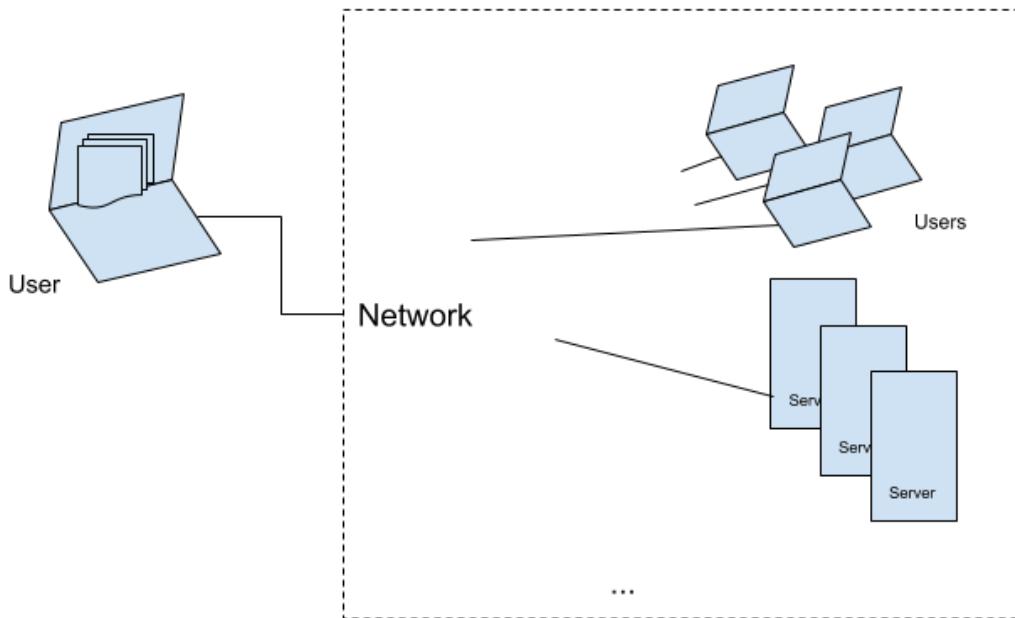


Figure 9 - Files located on one device

As a **second step**, you need to **assess** the damage that has been done. If you were complying to the principle of Confidentiality you will probably have a smaller and limited damage. In the case of a centralized file directory, this means that, if each one of your users had permission to access only few of the total data of the server and the attacker went through one user, then only his/her accessed files will be damaged. If you were complying to the principle of Integrity you could be sure about which files were damaged during the attack by comparing to a previous state of them (e.g. a recent backup). When assessing the damage, if you wish you can create a copy of your disk or the infected files for later on analysis.

The **third and final step** is about **Recovery**. In this Case Study, the principle of Availability suffered by the attack. The best practice to follow is to clean your system and then restore all of your data by using the most recent backups. To clean your system before restoring your data you can format and reinstall the operating system or you can try to disinfect your device by booting into safe mode and run your

antivirus software deep-scan. This will not help to decrypt your data, but it can clean your system from the infection so that the restored backup could be safely used. You can now understand the importance of regular backups. Hence, Availability is resolved. Don't forget to also restore the access to the server.

In the case that you don't have any backup available, then here is a list of some things you can possibly try [30], [31]:

- go back to a healthy system restore point if you have one;
- try to recover an older version of the files by using a shadow explorer software or a tool for data recovery;
- try to identify the specific ransomware type (there are some online tools available that can do that) and if identified, then check if a decrypt tool is already available for it and use it.

The above scenario sounds terrifying but it can be resolved relatively easy if you comply with the three principles and the solutions we have discussed throughout the chapter.



## E. Cybersecurity Checklist

	
Computers are backing up regularly	
Systems are updated regularly and timely	
Antivirus installed properly and according to the assessed needs	
Firewall installed	
Risk assessment completed and being monitored	
Follow a security framework in order to become more secure	
Establish a VPN Network for your users to use when needed	
Acquire a verified secure Certificate for your website (Https)	
Don't access websites characterised as insecure from your browser	
Using strong passwords and having them hidden from any unauthorised individual	
Supervise physical access to your premises and devices	
Confirm the identity of an email sender before providing any data or clicking on any files within the email	
Encryption of any sensitive data stored (e.g. using a dedicated software)	

Don't download untrusted software	
<b>Firewall Settings Checklist</b>	
Use a rule set with allowed services on your Firewall	
Inspect packet headers	
Enforce Rules	
<b>Network Monitoring Checklist</b>	
Use encrypted communication for serious transactions of your business	
Record and process network traffic	
Detect known attacks	
Detect anomalies	
Drop malicious traffic	



## F. Terminology glossary

**Asset:** we can consider as assets all the information, data, devices, computer systems, facilities and services that supports information-related activities. Thus, we can include in this definition the people also producing work on an information computer system. In the context of Cybersecurity, all assets need to be protected.

**Threat:** Any possible violation i.e. that could breach security and cause harm to the asset. It could be either intentional, accidental or even a subsequence of a natural disaster.

**Threat agent:** Any individual or entity wanting to do harm to an asset on purpose, or harms it accidentally e.g. someone unplugging a server by mistake or running physically into a system.

**Vulnerability:** a flaw or weakness in the design or implementation of an asset that could expose it to a threat or threat agent allowing him to use it to undermine the security. Examples can vary from as high-level issues as poor backups or as low level issues as poor coding.

**Exploit:** any software or tools intentionally used to take advantage of a vulnerability on an asset to cause malfunction or abnormal functionality one way or another. An obvious example can be the hacking tools.

**Firewall:** In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.

**Risk:** the probability that a threat will take advantage of a vulnerability on an asset and cause harm. As in all probabilistic theories, risk can be bigger or smaller based on some conditions. For example, we can say that there is bigger risk to lose some data if there exists only one backup, or there is bigger risk of someone attacking a bank data server instead of attacking a photo collection server.

**Attack:** any intentional event that harms or intends to harm an asset either by just obtaining it (passive attack), or by editing it, destroying it, removing it or even

revealing it without any authorised permission (active attack). Examples can be a denial of service attack, a data breach, or.

**Fault:** any accidental event that harms an asset, for example a physical destruction of equipment.

**Mitigation:** any tool, service or system that reduces the risk of attack.

**Compensating control:** any tool, service or system that reduce the risk of attack on an asset by intentionally getting in the way of the threat. An example is a firewall between the internet and the computer system.

**Associated individual:** the person relevant and connected to the information.

Glossary was created using definitions from [5] and also [12], [13], [14], [15], [16], [20]



## G. Conclusions

Maintaining a system secure over the web is a complicated issue, but can be faced through implementing some specific precaution measures, by following steps by step certified procedures and protocols and by applying certain solutions when a problem occurs.

Most importantly, all systems should at any time comply to the three main principles of the CIA triad: Confidentiality, Integrity, Availability. Unless you can say that you have covered the CIA triad on every system and process in your business, you are going to have issues at one time or another. To minimise any future problems and risk you have to think of the principles at every stage of the system life cycle, reassess your security regularly and every time it will become better than before.



## H. References

- [1] Gasser, Morrie (1988). Building a Secure Computer System (PDF). Van Nostrand Reinhold. p. 3. ISBN 0-442- 23022-2,
- [2] TechTerms - <https://techterms.com/definition/vpn>
- [3] Denial-of-Service Attack - [https://en.wikipedia.org/wiki/Denial-of-service\\_attack](https://en.wikipedia.org/wiki/Denial-of-service_attack)
- [4] <https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time>
- [5] Introduction to Cybersecurity for Business, University of Colorado System on Coursera, Taught by: Greg Williams, Lecturer Department of Computer Science
- [6] CS682: Advanced Security Topics Course by Dr. Elias Athanasopoulos, University of Cyprus (2018, <https://www.cs.ucy.ac.cy/courses/EPL682/>)
- [7] V-Alert Project, LLP Funded
- [8] <https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html>
- [9] <https://www.techrepublic.com/article/the-top-10-worst-ransomware-attacks-of-2017-so-far/>
- [10] <https://www.microsoft.com/en-us/download/details.aspx?id=12273>
- [11] <https://haveibeenpwned.com>
- [12] [https://en.wikipedia.org/wiki/Asset\\_\(computer\\_security\)](https://en.wikipedia.org/wiki/Asset_(computer_security))
- [13] [https://en.wikipedia.org/wiki/Threat\\_\(computer\)](https://en.wikipedia.org/wiki/Threat_(computer))
- [14] [https://en.wikipedia.org/wiki/Vulnerability\\_\(computing\)](https://en.wikipedia.org/wiki/Vulnerability_(computing))
- [15] [https://en.wikipedia.org/wiki/Exploit\\_\(computer\\_security\)](https://en.wikipedia.org/wiki/Exploit_(computer_security))
- [16] <https://www.techopedia.com/definition/6060/attack>
- [17] <https://www.avg.com/en/signal/what-is-malware>
- [18] <https://www.veracode.com/security/computer-worm>
- [19] <https://www.eugdpr.org/>
- [20] <https://www.techopedia.com/definition/1793/cyclic-redundancy-check-crc>

- [21] Furnell, S.M., Jusoh, A. & Katsabas D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, Vol.25: 27–35. Retrieved 10 March 2009 from <http://linkinghub.elsevier.com/retrieve/pii/S0167404805002038>
- [22] Whitten, A. & Tygar, J.D. (2005). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In: Cranor, L. & Garfinkel, S. (Eds.), *Security and usability: Designing secure systems that people can use*. Sebastopol, CA: O'Reilly, pp 669–692.
- [23] Flenchais, I. & Sasse, M.A. (2007). Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-Science. *International Journal of Human Computer Studies*. DOI:10.1016/j.ijhcs.2007.10.002
- [24] [https://uk.norton.com/norton-blog/2016/02/the\\_8\\_most\\_famousco.html](https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html)
- [25] <https://www.nist.gov/cyberframework>
- [26] <https://www.iso.org/isoiec-27001-information-security.html>
- [27] <https://www.cisecurity.org/>
- [28] <http://www.alphr.com/realworld/380632/how-to-deal-with-a-ransomware-attack>
- [29] <http://www.thewindowsclub.com/what-to-do-after-ransomware-attack>
- [30] <https://www.quora.com/How-do-I-use-my-computer-after-a-Ransomware-attack>
- [31] <https://www.tomsguide.com/us/ransomware-what-to-do-next,news-25107.html>
- [32] The European Union Agency for Network and Information Security (ENISA), Threat Landscape Report 2017, January 2018, p. 31-35
- [33] [https://en.wikipedia.org/wiki/Drive-by\\_download](https://en.wikipedia.org/wiki/Drive-by_download), access 27.01.2018
- [34] [https://en.wikipedia.org/wiki/Watering\\_hole\\_attack](https://en.wikipedia.org/wiki/Watering_hole_attack), access 27.01.2018
- [35] [https://www.rsa.com/content/dam/rsa/PDF/Making\\_Sense\\_of\\_Man\\_in\\_the\\_browser\\_attacks.pdf](https://www.rsa.com/content/dam/rsa/PDF/Making_Sense_of_Man_in_the_browser_attacks.pdf), access 27.01.2018
- [36] The European Union Agency for Network and Information Security (ENISA), Threat Landscape Report 2017, January 2018, p. 36-39

- [37] [https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection), access 27.01.2018
- [38] <https://www.acunetix.com/blog/articles/local-file-inclusion-lfi/>, access 27.01.2018
- [39] <https://www.acunetix.com/websitesecurity/cross-site-scripting/>, access 27.01.2018
- [40] <https://blog.udemy.com/php-injection/>, access 27.01.2018
- [41] <https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos>, access 27.01.2018
- [42] The European Union Agency for Network and Information Security (ENISA), Threat Landscape Report 2017, January 2018, p. 45-48
- [43] Zulfikar Ramzan, Phishing attacks and countermeasures, Mark Stamp, Peter Stavroulakis, Handbook of Information and Communication Security, Springer, <https://books.google.com/books?id=I-9P1EkTkigC&pg=PA433>, p. 433-447
- [44] The European Union Agency for Network and Information Security (ENISA), Threat Landscape Report 2017, January 2018, p. 64-67
- [45] <https://www.lifelock.com/education/how-common-is-identity-theft/>, access 27.01.2018
- [46] The European Union Agency for Network and Information Security (ENISA), Threat Landscape Report 2017, January 2018, p. 79-81
- [47] <https://www.pcworld.com/article/141474/article.html>, access 27.01.2018
- [48] <https://us.norton.com/internetsecurity-how-to-how-to-protect-your-new-tech.html>, access 27.01.2018

# SECTION V

## DIGITAL SECURITY RISK ASSESSMENT



## List of abbreviations

Abbreviation	Definition
DDoS	Distributed Denial of Service
DoS	Denial of service
ICT	Information and Communication Technologies
LFI	Local File Inclusion
PHPi	PHP injection or PHP Object Injection
RFI	Remote File inclusion
SQLi	SQL Injection attacks
XSS	Cross-site Scripting



## A. Introduction

Over the recent years digital security threats and various digital security incidents have greatly increased. Those various digital security threats and incidents cause real consequences, both economic and social, for the public sector, private organisations, not to mention individuals. Different examples of those consequences can be given, such as: financial loss, loss of customers or/and partners' trust, damage of organisation's reputation, disorder of organisational operations, etc. Nowadays the economic activities are highly connected and rely on data. Information and Communication Technologies (ICTs) and especially the Internet, are now essential to the functioning of the economy. Governments, public and private organisations, individuals today are dependant, in one way or another, on digital tools. Such issues as "Big Data" and "Internet of Things" provide a big potential of innovation regarding products and services. But they also have their impacts on the scale and scope of digital security. Not to mention the number of hacked websites every day and the number of viruses created every month. Strategies to manage digital security are needed and are essential to the economic and social activities. Therefore, the implementation of risk assessment procedures can help ensure digital security in both economic and social activities.

Risk assessment is a process of identifying, analysing and evaluating potential dangers which can be faced by an organisation and to impact its ability to conduct business. Risk assessment should also provide measures, processes and controls to minimise the impact of these dangers on current and future business operations [1]. To be able to carry out a Risk assessment, the organisation must identify the possible risks and determine the likelihood of such threats. Risk assessment is useful when: planning projects, improving safety of the workplace, preparing events, planning changes in the environment (new competitors, changes in government policies), etc. [2].

Digital economy allows organisations to increase and expand, but also due to fast pace of technology, it causes new security and privacy challenges. Digital security risks are a concern for both smaller entities as well as large organisations. Therefore, risk assessment is also the only way to ensure that the chosen cybersecurity controls

are fitting to the risks that an organisation is facing. In risk assessment an organisation estimates the probability of the risk occurring and the cost for an organisation if the risk happens [3], Digital Security Risk Assessment makes sure that time, efforts and resources are not wasted on implementing methods to defend against dangers that are unlikely to happen, or they will not have a significant impact on the organisation [4].

The digital ecosystem is nowadays essential to the economy and due to large-scale digital security incidents, OECD says that CEOs and governments should treat digital security as an economic risk: "Digital security risk should be treated like an economic rather than a technical issue (...)" [5]. This means that it is important to integrate Digital Security Risk Assessment in the organisation's overall risk management and decision-making processes.

The main objective of this chapter is to provide complete overview on Digital Security Risk Assessment approaches that should be followed by potential young entrepreneurs and young entrepreneurs in their digital business ventures and to highlight the importance of implementing Digital Security Risk Assessment strategies in online business ventures.

The chapter aims at equipping potential young entrepreneurs and young entrepreneurs in practical knowledge on the technical aspects (Digital Security as a Technical Risk) as well as on the economic aspects (Digital Security as an Economic Risk) of Digital Security. This chapter provides an overview of pros and cons resulting from implementing or not implementing Digital Security Risk Assessment.

Also, a practical advice is delivered and examples of good practices on how Digital Security Risk Assessment should be planned and carried out are outlined. This chapter includes also examples how Digital Security Risk Assessment strategy actually works and how it should be implemented on organisational level, to be a part of the organisation's overall Risk Management and Decision-Making Processes. Furthermore, possible shortcomings and gaps to be avoided are outlined, as well as approaches to overcome them.

The chapter provides a comprehensive terminology glossary, as well as a checklist of Digital Security Risk Assessment, as they are necessary in order to make complete knowledge on the topic available.



## B. Digital security as a Technical Risk

Having in mind the importance of Digital Security Risk Assessment and the need that Digital Security Risk Assessment should be a part of organisation's overall Risk Management and Decision-Making Processes, in this chapter we will focus on the technical dimension, as Digital security risk assessment has both technical and economic dimensions. This section describes the different technical risks regarding Digital Security and a selection of appropriate controls to treat the identified risks. The content is organised based on a contrasting juxtaposition of pros and cons as a result of implementing/not implementing such strategies.

There are many digital risks for the business and the organisations and they may result from different industries, sectors and may be of different sizes, as well as with differing security maturity. But all governments, public and private organisations, and also individuals, need to manage and mitigate their digital risks. Digital Security as a technical risk should also be of great importance to potential young entrepreneurs and young entrepreneurs in their digital business ventures. As a technical risk it poses threats to businesses, such as loss of economic assets and damaging their reputation.

This section describes the different technical risks in regard to Digital Security, related to: malware, web-bases attacks, web application attacks, phishing, spam, denial of service, ransomware, botnets, insider threat, physical manipulation, data breaches, identity theft, information leakage, exploit kits, cyber-espionage, which are described in detail in the chapter "Cybersecurity".

The listing above of different technical risks is a collection of current threats landscape in 2017, based on The European Union Agency for Network and Information Security (ENISA) "Threat Landscape Report 2017" [6].

Knowing the definition of **Malware**, available in the chapter "Cybersecurity" and the common types of malware, such as: viruses (which infects program files and/or personal files), worms (which can replicate itself across a network), spyware and keyloggers (which collect personal information of the user), Trojan horses (which look

and may even operate, as legitimate software), rootkit (which gains administrative rights to the operating system for malicious intent), browser hijackers (which modifies web browser settings), malvertising (the use of legitimate online advertising systems, in order to spread malicious software), lets now describe the different technical risks in regard to this aspect of Digital Security [7].

When the threats listed above are present on a device or are being transmitted over a network, they can drain the device or network resources and slow down the Internet connection. There are also other technical risks arising from those threats, as malware can:

- destroy or corrupt your personal or business files,
- deactivate antivirus software or even hinder the functions of your web browser, to prevent you to download virus removal tools,
- collect keystrokes, which can be used to stealing credit card numbers and passwords,
- hijack your web browser or device in order to: use it maliciously or commercially or direct you to website, which try tricking you to enter passwords to your accounts,
- send copies of itself to your email contacts [8].

Below you can find a selection of most important appropriate controls to prevent and treat the identified risks, coming from malware:

- use only licensed copies of software and/or download software from known and trustable sources,
- install only software which is needed on a device, as extra un-used software causes an extra threat,
- store original copies of software in a safe location,
- back-up your files and system regularly and store copies in a safe location,
- update regularly your: operating system, web browser, antivirus definitions, antispyware, all other installed software,
- do not use software, disks, portable disks, etc. from home systems.

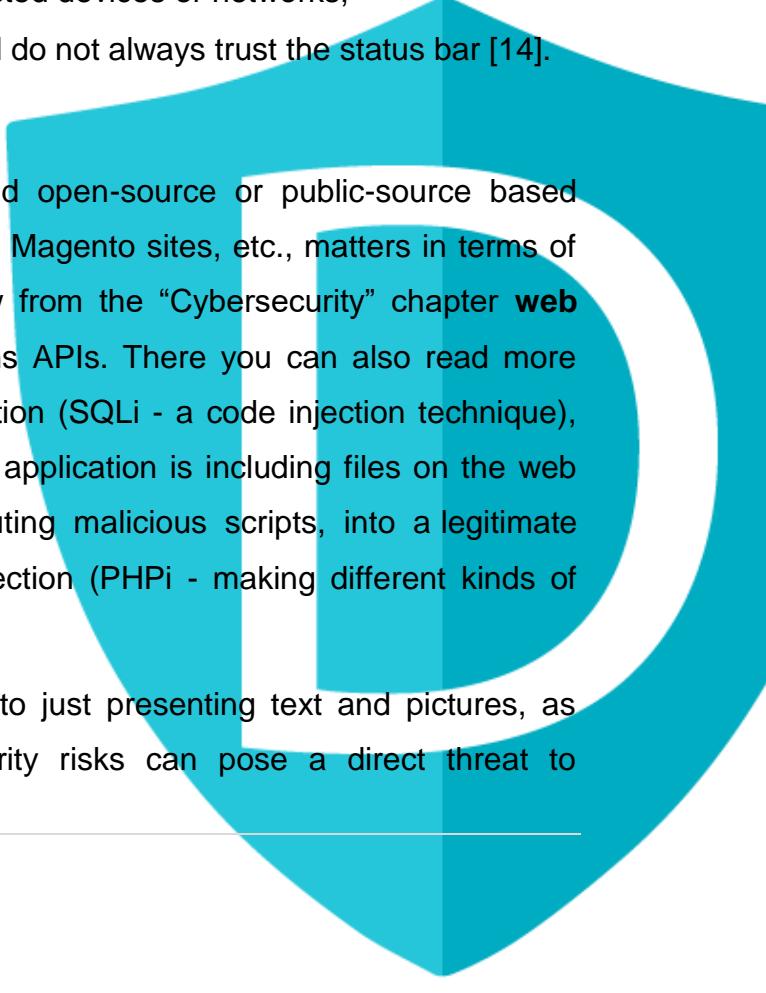
**Web-based attacks** which make use of web-enabled systems and services, are also described in chapter “Cybersecurity”. After reading that chapter you are already familiar with different types of those attacks, such as: web browser exploits (malicious code that use vulnerability in an operating system or an installed software), web servers and web services exploits (taking advantage of a bug or vulnerability of a web server or web services), drive-by attacks (unintended download of computer software from the Internet), water-holing attacks (infecting selected websites with malware), man-in-the-browser-attacks (intercepting sensitive information and data). Now we can describe the different technical risks in regard to this aspect of Digital Security:

- web browser exploits can perform for example an address bar spoofing, meaning that the user sees a trusted URL (for example online bank) in the bar, but the content of the website is controlled by the attacker. This can be used to steal login and access information [9],
- web servers and web services exploits can for example use the Cross Site Scripting vulnerability, meaning that attacker can execute malicious scripts, into a legitimate website or web application. This can be used to collect data from the page, hijack user sessions, redirect users, collect information about the user that is viewing the website [10],
- drive-by attacks can install keyloggers, ransomware on a device or even create a backdoor which enables the attacker to install even more malware. This can be used to encrypt data on a device and demand a ransom and collect keystrokes or search for passwords, account information and other sensitive information, in order to gain unauthorised access or conduct unauthorised transactions [11],
- water-holing attacks are used to attack a profiled group of users, by malicious code, with the intention to steal data or take control over systems of an organisation, industry or in a region (a profiled group). This can lead to threats at multiple organisations, including health, technology, educational, government, etc. [12]
- man-in-the-browser-attacks are often used to steal one-time password codes (SMS), which banks use to authenticate a user’s money transfers. When the device is infected with a man-in-the-browser trojan and the user navigates to an

online banking website, this session triggers the trojan, which can change the account number and/or bank transfer amount, in the same time displaying a website with the legitimate transaction details to a user [13].

As we can see above Web-based attacks are often used to: steal login, passwords and other access information/one-time password codes, in order to gain unauthorised access to systems or conduct unauthorised transactions via on-line banking. They cause a major threat both to users and organisations, so it is important to take appropriate controls to prevent and treat the identified risks. Here is what you can do to prevent and treat those risks:

- install anti-virus and anti-spyware software and keep it updated,
- always keep your operating system and web browser updated,
- configure security options in your web browser (for example: use a pop-up blocker, don't save your passwords and form information),
- use the Internet being logged on your computer as a user that does not have administrative rights,
- view e-mails in plain text, not as HTML view,
- use a pre-paid credit card when purchasing on the Internet,
- do not use your on-line banking on untrusted devices or networks,
- type in the website address manually and do not always trust the status bar [14].



Also, the popularity of such resources and open-source or public-source based projects, as Joomla and Wordpress plugins, Magento sites, etc., matters in terms of Digital Security. As you already may know from the "Cybersecurity" chapter **web application attacks** abuse web applications APIs. There you can also read more about the types of such attacks: SQL Injection (SQLi - a code injection technique), Local/Remote File Inclusion (LFI/RFI - web application is including files on the web server), Cross-site Scripting (XSS - executing malicious scripts, into a legitimate website), PHP injection or PHP Object Injection (PHPI - making different kinds of malicious attacks).

Web applications are not limited anymore to just presenting text and pictures, as a paper brochure. Web applications security risks can pose a direct threat to

organisations, as today all personal and business users use web applications on a daily basis. Web applications are the crucial tools that allow private users, organisations, customers and even countries to communicate, access, and process information. That information can include for example: financial information, medical records, national security data, etc. [15].

Here are some technical risks in regard to this aspect of Digital Security:

- breaching a system's protection mechanisms,
- gaining information that should not be available outside the application or/and organisation (for example Intellectual property),
- gaining unauthorised access to web applications and stored data (for example: names, credit card numbers and any other sort of confidential and sensitive commercial data),
- browser spying (cookies manipulation can allow unauthorised user to pretend to be a legitimate user),
- elevation of privileges to an authorized user,
- identity theft, theft of service or content, and credit card fraud,
- denial of service.

As web applications evolved and securing web applications has become important, we need to list the most important appropriate controls to prevent and treat the identified risks:

- a risk management program is essential, policies and procedures should stop the deployment of web applications with vulnerabilities,
- training developers in secure coding practices,
- web applications must be tested by professional security testers, before deployment [16],
- updating security patches for web servers and applications,
- using Intrusion Detection Systems (IDS) and Intrusion Prevention systems (IPS),
- using advanced firewalls (which offer the ability to drop malicious packets),
- scanning for coding vulnerabilities after an application has been built, with specialised software,
- using web server scanners to look for dangerous files on web servers. [15].

Also, it is important to highlight that such issues as:

- orphaned web applications (developed by teams which are no longer with the company or web applications which are not maintained anymore),
- legacy web applications (old web applications created before security policies were put into practice),
- short time to market deployment of web applications,
- custom-made web applications (in-house-developed web applications are subjected to high human error),
- increase web applications security risks [17].

As **phishing** is unfortunately a very popular Internet fraud, it is important to include phishing in the Digital Security Risk Assessment.

A successful phishing attack can lead to such technical risks as:

- using your computer to install viruses and worms,
- sending phishing emails to all your email contacts,
- using stolen data to access organisation's system, breaching system's protection mechanisms,
- using stolen personal data to open fake bank accounts or credit cards and then use them in illegal transactions,
- using your on-line banking system account to make frauded bank transfers or on-line purchases.

The above technical risks can lead to such economic risks, as: financial losses, reputational damages.

To reduce the above risks, such controls should be implemented:

- identify departments which are most likely to be harmed by phishing,
- develop a phishing protection and response plan,
- communicate the plan both to your organisation employees and external parties (partners, costumers, etc.),
- train your employees [18].

**Spam** can be sent by botnets or virus infected computers, but also spam is a problem on social media, such as: Facebook, Twitter and LinkedIn. With spam attacks on social media scammers can gain access to user's profile pages, on which they can post disturbing links, images or videos. Spam is also an issue on instant messaging in social media. We can observe that spammers are moving from email to social media. So exactly what are the technical risks from spam:

- infecting computers, web applications, servers and networks with viruses and/or malicious code,
- spam emails take up storage space on email servers,
- spam emails can generate a large number of server requests and sometimes can even cause a server-failure, leaving the organisation without email,
- devices, infected with the use of spam, can become part of a botnet, launch malware, send spam or take part in Distributed Denial of Service (DDoS) attacks.

Organisations can protect themselves from spam and various negative consequences coming from spam:

- use anti-spam engine on your email servers and keep it always updated, anti-spam engine should scan all inbound and outbound emails for spam and malware,
- anti-spam engine should use such techniques as: reputation filtering or pattern matching, to detect new and emerging campaigns,
- setting up alerts when organisation's email server has become part of a botnet, to ensure organisation's infrastructure is used only in a legitimate way [19],
- also, users should be educated: not to reply to spam emails, not to click any links or download/open files in a spam email, not to forward an email from someone he/she doesn't know, to use a spam filter, to report spam [20],
- on social media you should: not use applications that you do not trust, beware of suspicious link posted on social media or sent by instant messaging,
- always delete from your social media account apps that you do not know,
- delete all posts/messages posted/sent on your behalf by apps and notify your contact that you might have been sending spam [21].

As most organisations use web applications and server infrastructures as their regular operations, protecting web applications and server from **Denial of service (DoS) attacks and Distributed Denial of Service (DDoS) attacks** is something that organisations need to take care of. DoS or DDoS attacks deny employees, members or account holders, so actual legitimate users, of the service or resource. But those attacks have also other technical risks:

- high bandwidth or computing power consumption,
- they focus the IT staff on resolving this issue, as the attacker may carry-out a different attack focusing for example on stealing data,

as well as non-technical risks connected with revenue loss and damage to organisations' reputation [22].

What should be a response to a Denial of service (DoS) attack and Distributed Denial of Service (DDoS) attack and how reduce the risk from such attacks:

- absorbing the attack, using a firewall, is the simplest response,
- possibility to limit: incoming traffic from certain IP regions, number of baskets that users can create, number of enquiries to search feature on a website,
- making websites, web application and system more efficient, in terms of processing power,
- encouraging best practice in coding (for example to stay secure from overwhelming the website with search queries),
- using monitoring tools, to analyse the incoming traffic and identify the malicious requests,
- find out in advance which measures the service provider, web-hosting company can take during a DoS/DDoS attack [23].



In the “Cybersecurity” chapter and also previously in this chapter we have mentioned the word **botnet**. But what are the technical risks coming from this threat - when a device is infected:

- boots drain the device computing power or network resources, to carry out the attacker’s tasks,

- high bandwidth consumption,
- stolen sensitive data,

as well as non-technical risk connected with high bandwidth costs and damage to organisations' reputation, both when their infrastructure runs or is a target of a botnet.

Organisations can take different measures to prevent botnet risks:

- monitoring of network performance and network traffic, to detect irregular network behaviour,
- all networks', servers' and devices' software should be updated regularly,
- using anti-botnet tools (firewalls, antivirus software, rootkit detection packages, network sniffers, and specialized anti-bot programs) to find and block bot viruses,
- removing the bot viruses fast and eliminating the security vulnerability,
- also, users should be educated: not to click any links or download/open files in a spam email [24].

Another threat in the cybersecurity landscape are **insider threats**, which we are also addressed in chapter "Cybersecurity". Why those threats are so important? There are many reasons, but we should mention at least:

- it is hard to detect intentional actions, as it is hard to distinguish them from a nonthreatening activity - regular work of employees,
- usually malicious employees know how to cover-up their actions, making it hard to prove their guilt (they will try to explain it was a mistake).

So how to spot such malicious employees:

- employees downloading data to external drives,
- employees accessing data not relevant for their work,
- employees emailing data to personal emails accounts,
- employees requesting higher-level access without the need for it,
- employees often accessing the office outside their working hours,
- employees violating organisation's policies,
- employees making too much use of printers and scanners,
- employees installing software not relevant for their work,

- employees attempting to access restricted areas [25].

**Data breach** and **Identity theft**, as a special case of data breach, are serious consequences of many of the above-mentioned issues connected with Digital Security risks. Both topics have been addressed in the “Cybersecurity” chapter. In this chapter we are listing a selection of appropriate controls to prevent those risks:

- develop and implement a data loss protection plan,
- educate employees regarding data procession and protection, also provide technical support,
- don't collect data that you don't need,
- don't store data in many places,
- keep your applications and systems always updated,
- remember that data encryption should not be the only method of your defence,
- require the same standards from your vendors and partners [26].

A special focus should be also put to reducing the risk of becoming a victim of identity theft, you should:

- reduce the number of credit and debit cards you have,
- reduce the number of financial institution which services you use,
- use a prepaid card then shopping online,
- never give out your credit or debit card number, personal information, over the phone, by mail or on un-secured websites,
- contact the issuer of your credit or debit card, when you expect a new or reissued card to arrive and it is not in your mail-box,
- annually check your credit reports [27].

Unfortunately, you can't protect yourself completely and if a thief wants to steal your information, his or her chances are extremely high [28].

### C. Digital Security as an Economic Risk

Knowing the technical dimension of the Digital security risk, its economic dimension needs to be further elaborated. This section explains the impact of Digital Security on the economic dimension, as such special focus to economic and social activities is needed, rather than to look at the risk solely from digital infrastructure perspective.

The Digital Security economic dimension should also be of great interest to potential young entrepreneurs and young entrepreneurs in their digital business ventures, as digital security risk should be treated like an economic rather than just a technical issue. This means it is important to integrate digital security risk assessment procedures in the organisation's overall risk management and decision-making processes. All stakeholders, including potential young entrepreneurs and young entrepreneurs, should be aware that digital security risks can affect the achievement of their economic and social objectives. Especially potential young entrepreneurs and young entrepreneurs should be empowered with the education and skills necessary to understand this risk and the impact of their digital security risk management decisions on their business activities. Further they should be aware that they can't protect themselves completely, so they must handle a certain level of digital security risks, in order to achieve their economic and social objectives. Also, digital security risk management should respect interests of other parties and the society as a whole [29].

Digital security can be approached from at least four different perspectives, such as: technology, law enforcement, national and international security and also economic and social prosperity. As this section explains the impact of Digital Security on the economic dimension, the next includes "wealth creation, innovation, growth, competitiveness and employment across all economic sectors, as well as other aspects, such as: individual liberties, health, education, culture, democratic participation, science, leisure, and other dimensions of well-being in which the digital environment is driving progress" [30]. It is because the digital environment is essential to the functioning of today's economies and societies and is the source of innovation.

Digital security incidents cause different consequences for the affected organisations, such as undermined reputation (when the organisation's brand is exposed), loss of competitiveness (when trade secrets are stolen), financial loss resulting from the attack itself (for example sophisticated scam schemes), from lost business, disruption of operations (for example sabotage), recovery costs or legal proceedings and fines. It is also difficult to assess the actual costs of digital security incidents, as often organisations do not share those kind of information, as they are viewed as potentially damaging information. Because of this, there is no statistics or data sources regarding the real costs of digital security incidents. "Breached organisations can end up paying fines, legal fees, and redress costs". Another economic consequence of digital security risks are the changes in the organisations' management after such incidents. In the past many CEOs or Directors stepped down and different levels executives lost their jobs, as a result of a security breach, which was disclosed by media. Also, individuals and small and medium sized companies can experience financial loss, identity theft and also other economic impacts, due to data breaches. Individuals as consumers can also lose confidence in the whole sector/system, not only the trust to an individual affected institution [31].

Organisations and especially potential young entrepreneurs and young entrepreneurs should ensure that their digital security measures will support economic and social activities. It is impossible to eliminate every potential risk, so certain decisions have to be made, taking into account that a digital security measures "can increase financial cost, system complexity and time to market, as well as reduce performance, usability, capacity to evolve, innovation, and user convenience". All of the mentioned issues are costs. [32].

Managing digital security risks requires taking into account that such risks actually do exist and certain skills, which can be acquired by education (some of those skills can be gained via our e-Manual), practice, experience and each of these are further costs for the organisations.

## D. Integrating Digital Security as part of an organisation's overall Risk Management and Decision-Making Processes

Knowing the different technical and economics risks, we should see a clear need in integrating Digital Security as part of an organisation's overall Risk Management and Decision-Making Processes.

**But what does risk exactly mean?** We can think of the following example: a client has made an order from our online shop half an hour before noon, and our delivery policy says that if someone orders before noon, then they will have their order delivered on the same day. We are in a hurry to issue and print the invoice, to be able to give the parcel to the courier before he/she leaves for the afternoon deliveries, in order to have the order delivered on time and therefore comply to our policy. This is an everyday, very possible to happen “emergency” situation. The risk of the Internet going down exists, and that will prevent us from issuing the invoice from our online shop. There is also the risk of the devices (computer or printer) going down so we will not be able to print the invoice. This is not a huge security crisis, but it can lead to customer dissatisfaction, cancellation of the order and eventually loss of good reputation.

A good way to analyse and understand risk is by breaking it in the following areas:

- a) **What** we access might increase the risk of compromising security. Do we know if the websites we access through Internet surfing are safe? Sometimes when you visit a website, you may get a notice from your browser that this website has an untrusted certificate. You have the option to either proceed or leave. What shall you do?

What about software? Do we know that the software we want to install is secure? Even if it is absolutely secure, is it possible that we have too many applications installed on our devices that slow down the performance? Or is it possible that we don not have access to the best software for the tasks we need to do and that would make us less productive? Do we connect our personal devices to the

business network? Do we do non-business use of the companies computing devices? Are we accessing or downloading illegal material?

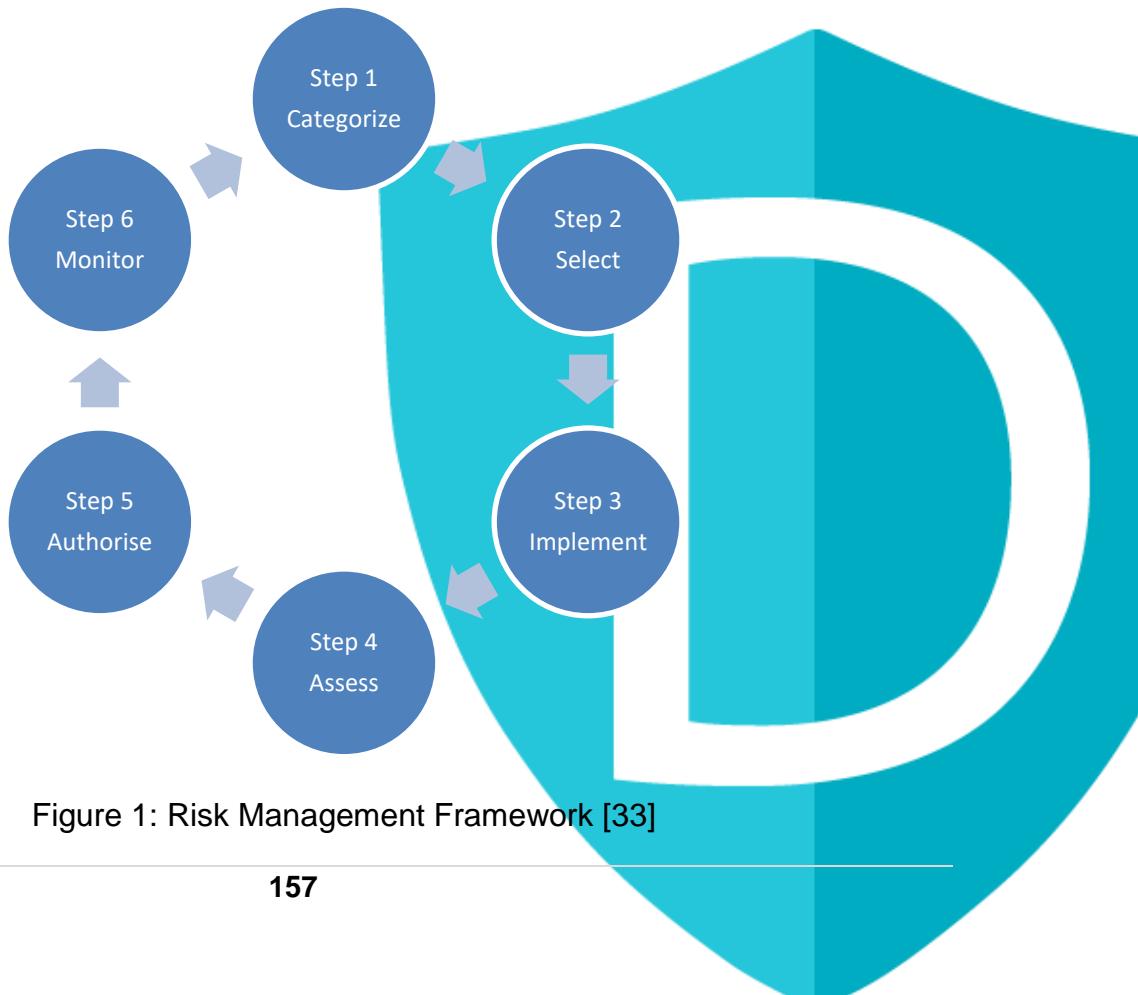
- b) **Where** we connect can increase the risk of compromising the integrity and confidentiality of our systems. Can we be sure that the network that we are connected to is trusted? Using our mobile devices on untrusted networks like the airport Wi-Fi, or just the simple example of connecting to a coffee shop could be unsafe and harmful to our data and our devices.
- c) **When** events happen, risk increases. For example, if there is a big catastrophic physical phenomenon and you receive an email stating that it is from the red cross and they are accepting donations can we believe that right away? We will have to cross check it a little bit first.
- d) **How** do we adhere to security best practices? Do we follow the best practices? Do we have enough knowledge before doing something? If not, then we will have to do research and learn more before acting. More knowledge equals less risk.
- e) **Why** do we use these best practices? We must be able to logically reason and know about any measures we take concerning cybersecurity. Don not just follow the crowd or what is written in a single website. Investigate, research, ask, learn, understand. Maybe some measures will be good for your company, or maybe they will be harmful. Knowing why you do something, decreases the risk. For example, when you receive a link to click or an email to read, do not just do it without understanding why. Another example is the unnecessary use of file sharing services for storing data just because it is easier, without knowing the threats that may exist. What if your password is stolen, or what if you forget forever all of your credentials?

Furthermore, to understand the risk you have to also take into account some factors of risk that you will not be able to change. For example, you will not be able to change the way operating systems or purchased software work and the vulnerabilities they have. You will only be able to enhance them with other measures. There might be users that will refuse to follow the best practices that you will set for your business security. You will have to deal with them in a different level, without compromising security measures or cybersecurity.

To manage operational and organizational risk, you can make use of a **Risk Management Framework**; a workflow of process to help in their management. But what is the difference between Operational and Organizational Risk. Operating services, systems or functions within the organisation relate to Operational Risk, whereas, the overall architecture of the organisation as a whole relate to Organizational Risk. In the Risk management framework Security and risk management activities are integrated throughout the entire system or service life-cycle, which is a significant step in providing an effective information security program.

An internal part of the overall strategy for your business/organisation must be Risk Management. It will help you answer questions such as "How do you identify risk?" and "How do you deal with it?". NIST 800-37, which is a framework for ongoing and real-time risk management for system life-cycles, is a good example.

Well, how do you set up a risk management framework? The Risk Management Framework Life-Cycle provides a series of steps that can be applied in order to setup your own Risk Management Framework (see Figure 1). These steps are briefly presented next.



**Step 1:** Categorize/Define the system and how it is used. The importance of the system must also be considered, e.g. is it a server with photos or a credit card system? In the case that it is a credit card system, is it a credit card server or terminal? In the case they are down, how can we deal with them being down? You will need to assign roles for who is a responsible in this step (e.g. system owner).

**Step 2:** Select the security controls that will be placed on the system based on criticality (i.e. low, medium and high). Be aware that high criticality cannot be assigned to all the security controls. As previously mentioned, it is not good practice to have security controls on everything since it can result in performance issues, e.g. antivirus requirements will need to be determined for employee workstations or determine if employees require specific authentication to access financial systems (of course there is). Again, you will need to assign roles for who is a responsible in this step (e.g. information security officer).

**Step 3:** Following the selection of security controls in Step 2, you will need to implement them in this step (e.g. install the selected antivirus on systems). You will need to assign a responsible person in this step as well (e.g. information system owner).

**Step 4:** Following the implementation of information security controls in the previous step, you will need to develop several processes in this step to ensure that they are in place and not affected, e.g. checking that your antivirus does actually protect your system(s) against threats or considering new threats to protect against, which were not initially considered. You will need to assign roles for who is a responsible in this step as well (e.g. auditing/information security office in your business/organisation or third-party company).

**Step 5:** Assuming that you have already identified a risk, what actions will you take to mitigate it? Furthermore, is it possible to apply those actions you have in mind? Is there any reason why you would accept a risk (in the case that you are authorised to take such actions), e.g. certain antivirus cannot be

installed on point of sale terminals? Hence, will you accept the risk of having no antivirus or will you search for a compromising solution. You will need to assign roles for who is a responsible in this step as well (e.g. auditing/information security office in your business/organisation).

**Step 6:** Continuously monitoring the information system and security controls applied for their effectiveness occurs in the final step of the life-cycle process. A common method is to log every single system action, network traffic packet, system transaction, user sessions, etc. This is referred to as logging and will help you monitor for identified risks or breaches on the entire system by reviewing the log files. This enables one to take immediate actions where necessary. You will need to assign roles for who is a responsible in this step as well (e.g. many different people or domain specific specialists in your business/organisation) [33].

Deciding on a suitable Risk Management Framework requires wise consideration. You need to construct a complete framework that will work for your business environment.

A significant role in the process of a Risk Management Framework is attributed to **Risk Assessment**. Risk Assessment process is composed of several steps: prepare for the assessment, conduct the assessment, communicate assessment results and maintain the assessment. Figure 2 illustrates these steps. Risk Assessment process is further elaborated below.

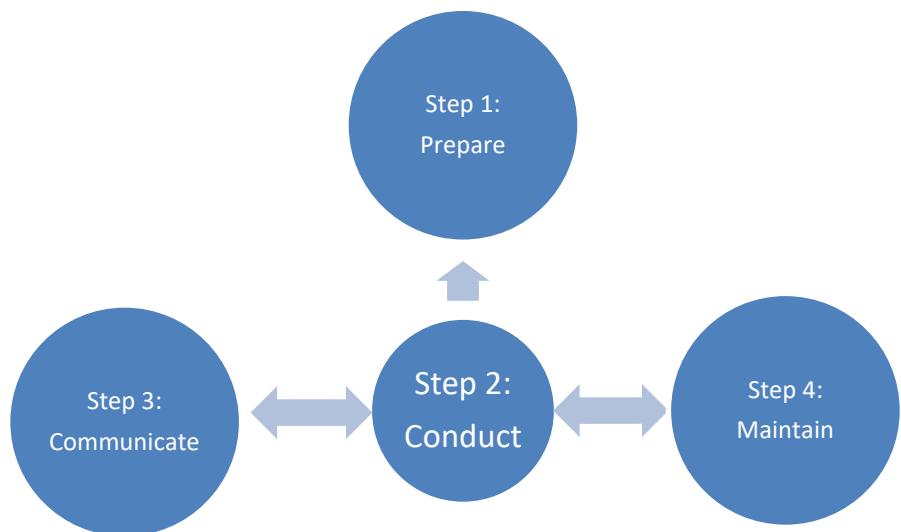


Figure 2: Risk Assessment [34]

**Step 1: Prepare for Assessment.** First identify the purpose of the assessment.

Think about things like what the assessment aims to cover; what is the scope. Assumptions and constraints associated with the assessment will need to be defined. Moreover, sources of information that you will need to use as inputs for the assessment need to be declared. Final action is determining the risk model and analytic approaches.

**Step 2: Conduct Assessment.** Consider threat sources and events that could be produced by them. Follow this up by detecting vulnerabilities within your business/organisation systems, which entails following a specific plan made possible by threat events and predisposing conditions that could affect exploitation. Next, the likelihood of identified threat sources producing and executing specific threat events must be determined, assuming those threat events will be successful. Side effects will then need to be determined; impact being on organizational operations and assets, individuals, other organisations or even at national level. This can be caused by the exploitation of vulnerabilities via threat sources through specific threat events. Clarifications are needed on which security risks can be found as a

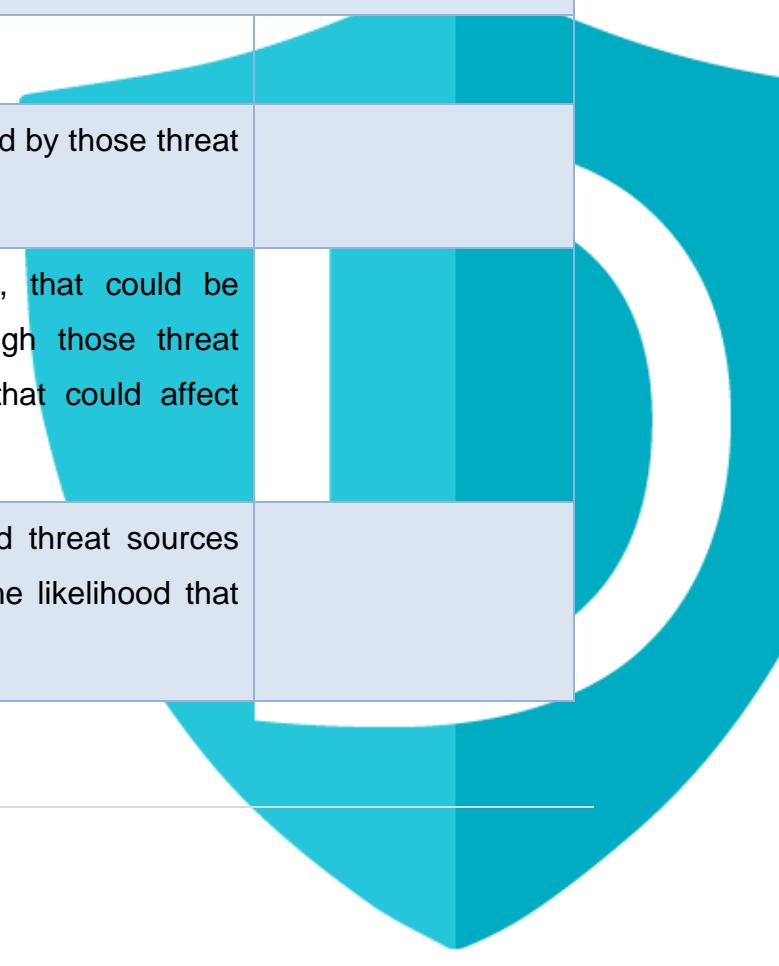
combination of possible threat exploitations of vulnerabilities and on what their impact is, including any uncertainties associated with the risk determinations.

**Step 3: Communicate results.** The results of the assessment must be well understood. Only then you can share them together with the information that was used as an input in the beginning of the assessment. In communicating the results, you will support other risk management activities.

**Step 4: Maintain results.** Risk factors that were determined during risk assessments must be monitored continuously in order to understand any subsequent changes to these. Remember to update the components of risk assessments so they reflect the monitoring activities carried out by your organization [34].



## E. Digital Security Risk Assessment Checklist



<b>Step 1: Preparing for the Risk Assessment</b>	
Identify the purpose of the assessment	
Identify the scope of the assessment	
Identify the assumptions and constraints associated with the assessment	
Identify the source of information to be used as inputs to the assessment	
Identify the risk model and analytic approaches to be employed during the assessment	
<b>Step 2: Conducting the Risk Assessment</b>	
Identify relevant threat sources	
Identify threat events that could be produced by those threat sources	
Identify vulnerabilities within organisation, that could be exploited by those threat sources, through those threat events and the predisposing conditions that could affect successful exploitation	
Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful	

Determine the adverse impacts to organisation's operations and assets	
Determine digital security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation	
<b>Step 3: Communicating and sharing Risk Assessment Information</b>	
Communicate the risk assessment results	
Share information developed in the execution of the risk assessment	
<b>Step 4: Maintain the Assessment</b>	
Monitor risk factors identified in risk assessments on an ongoing basis and understanding	
Subsequent changes to those factors, update the components of risk assessments reflecting the monitoring activities [34]	



## F. Terminology glossary

**Risk** - the potential of gaining or losing something of value [35].

**Risk Assessment** - the process of identifying the risks related to a well-defined situation and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact. Part of Risk Management and synonymous with Risk Analysis [34].

**Risk Management** - the total process of identifying, controlling, and mitigating risks. It includes risk assessment [34].

**Threat** - the potential for a threat-source to exercise a specific vulnerability [34].



## G. Conclusions and Further Reading

Having read the above, you now know how important it is to integrate Digital Security Risk Assessment in the organisation's overall risk management and decision-making processes. In this chapter we presented a complete overview on Digital Security Risk Assessment approaches that should be followed by potential young entrepreneurs and young entrepreneurs in their digital business ventures and highlighted the importance of implementing Digital Security Risk Assessment strategies in an online business venture. We aimed on providing knowledge on both the technical aspects (Digital Security as a Technical Risk), as well as on the economic aspects (Digital Security as an Economic Risk) of Digital Security.

Further we consider and advise further reading as necessary in order to have complete knowledge on this topic.



## H. References

- [1] <http://searchcompliance.techtarget.com/definition/risk-assessment>, access 13.11.2017
- [2] [https://www.mindtools.com/pages/article/newTMC\\_07.htm](https://www.mindtools.com/pages/article/newTMC_07.htm), access 13.11.2017
- [3] <http://www.genre.com/knowledge/blog/steps-to-a-good-risk-assessment-en.html>, access 13.11.2017
- [4] <https://www.itgovernance.co.uk/cyber-security-risk-assessments-10-steps-to-cyber-security>, access 13.11.2017
- [5] <http://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm>, access 13.11.2017
- [6] [https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at\\_download/fullReport](https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at_download/fullReport), access 27.01.2018
- [7] <https://www.lifewire.com/what-is-malware-2625933>, access 27.01.2018
- [8] <https://oit.ncsu.edu/it-security/safe-computing/viruses/>, access 16.05.2018
- [9] <https://www.trendmicro.com/vinfo/us/security/definition/address-bar-spoofing>, access 16.05.2018
- [10] <https://www.acunetix.com/websitedevelopment/cross-site-scripting/>, access 27.01.2018
- [11] <https://www.lastline.com/blog/drive-by-download/>, access 16.05.2018
- [12] <https://searchsecurity.techtarget.com/feature/Targeted-Cyber-Attacks>, access 16.05.2018
- [13]  
[https://www.rsa.com/content/dam/rsa/PDF/Making\\_Sense\\_of\\_Man\\_in\\_the\\_browser\\_attacks.pdf](https://www.rsa.com/content/dam/rsa/PDF/Making_Sense_of_Man_in_the_browser_attacks.pdf), access 16.05.2018
- [14] <https://www.sans.org/reading-room/whitepapers/application/web-browser-insecurity-1637>, access 16.05.2018
- [15] <https://www.sans.org/reading-room/whitepapers/application/web-based-attacks-2053>, access 16.05.2018

[16] <https://www.business.att.com/learn/operational-effectiveness/the-top-10-web-application-security-risks.html>, access 16.05.2018

[17] <http://www.trendmicro.it/media/misc/web-application-vulnerabilities-en.pdf>, access 16.05.2018

[18] <http://resources.infosecinstitute.com/category/enterprise/phishing/phishing-as-a-risk-damages-from-phishing/#gref>, access 16.05.2018

[19]

[https://www.bloxx.com/media/1356/bloxx\\_whitepaper\\_increasingemailthreats\\_us.pdf](https://www.bloxx.com/media/1356/bloxx_whitepaper_increasingemailthreats_us.pdf), access 17.05.2018

[20] <https://www.techsoup.org/support/articles-and-how-tos/things-you-can-do-to-prevent-spam>, access 17.05.2018

[21] <https://www.facebook.com/help/217854714899185>, access 17.05.2018

[22] <https://www.quora.com/How-dangerous-is-a-DDoS-attack>, access 17.05.2018

[23] <https://www.computerweekly.com/feature/DDoS-attack-threat-cannot-beignored>, access 17.05.2018

[23] <https://www.computerweekly.com/feature/DDoS-attack-threat-cannot-beignored>, access 17.05.2018

[24] <https://www.veracode.com/security/botnet>, access 17.05.2018

[25] <https://securityintelligence.com/the-cisos-guide-to-managing-insider-threats/>, access 17.05.2018

[26] <https://www.kroll.com/en-us/what-we-do/cyber-security/prepare-and-prevent/cyber-risk-assessments/data-breach-prevention-tips>, access 17.05.2018

[27] <https://www.privacyrights.org/consumer-guides/how-reduce-your-risk-identity-theft>, access 17.05.2018

[28] <https://www.thebalance.com/prevent-identity-theft-1947624>, access 17.05.2018

[29] OECD, Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, <http://dx.doi.org/10.1787/9789264245471-e>, p. 9

[30] OECD, Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, <http://dx.doi.org/10.1787/9789264245471-e>, p. 19-20

[31] OECD, Managing Digital Security and Privacy Risk for Economic and Social Prosperity, OECD Publishing, [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG\(2016\)1/FINAL&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2016)1/FINAL&docLanguage=En), p. 14-15

[32] OECD, Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, <http://dx.doi.org/10.1787/9789264245471-e>, p. 35

[33] <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-37r1.pdf>, access 11.06.2018

[34] <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>, access 11.06.2018

[35] <https://en.wikipedia.org/wiki/Risk>, access 11.06.2018



## Thank you from the DiFens team

We hope that this e-Manual served its purpose by helping you ease into the world of digital security for your current or future enterprises and pointing you in the right directions.

Feel free to further explore the topics covered on one side by the Further reading chapters in every e-Manual section, as well as through finding additional literature, relevant to your own field of operations.

If or when you need some additional guidance, you can seek mentoring in the topics of entrepreneurship and digital security in the DiFens mentoring platform, available to be accessed at <http://www.difens.eu/>. When you feel confident enough yourself, you can also become a mentor and help other young entrepreneurs in their endeavours by sharing your knowledge and experience with them.

For more information about the project and the team behind it, visit <http://difens-project.eu/> or contact us at [difensproject@gmail.com](mailto:difensproject@gmail.com).

Thank you for joining us and we wish you the best of luck in securing your enterprises!