Cyber Security Framework

Assignment 1

21321906 | Computer Security | CP60028E 2019

Contents

Table of Figures

Abstract

The national cybersecurity landscape has changed profoundly in recent years by acquiring greater awareness of cyber risk and the need for adequate security measures.

In this context, a Computer Security Framework is presented, a result of literature research in academy and security private companies. This Framework, inspired by the CIS (Centre for Internet Security), the ISO 27000 and the CoSO standards provide an operational tool for organising security processes suitable for organisations of any size working in the travel industry.

The UK travel sector landscape is constituted, in the vast majority, by small and medium companies, in which specific staff that systematically deal with cybersecurity practices is not present due to structural and turnover issues. For these reasons, it is critical to address security problems which, if not prevented or acted upon, may lead to disastrous financial consequences. To answer to these needs, this Cyber Security Framework describes the most popular security threats, necessary countermeasures and controls that are easy and, almost always, economical to implement and that represent security practices that cannot be ignored.

On 25 May 2018, two years after its entry into force, the Regulation General on Data Protection (GDPR - further on in this document also indicated merely as a Regulation) [1] became operative to govern the processing and circulation of personal data.

The Regulation imposed a change of perspective concerning the protection of personal data by introducing the principle of accountability. More than 11 months from the full application of the Regulation its implementation represents a fundamental step for any organisation that intends to process personal data.

In recent years, cyber threats have further evolved in quality and quantity. Today a fundamental problem is represented by data breaches that fraudulently subtract data, also sensitive ones, from the databases of industries, public bodies and organisations of each kind. Data breaches are often significant damage to, and today, in the light of the rules provided by the Regulation, they can be the cause of substantial fines.

This document proposes a Framework for Cybersecurity and Data Protection (from now on referred to as the Framework only) to support organisations that need strategies and processes aimed at protecting personal data and information security.

This document introduces contributions aimed at capturing the fundamental aspects related to data protection under the Regulation, standards and legal Acts.

Note that the Framework is a support tool for the organisation and cannot in any way be considered a tool for compliance with current regulations. Nevertheless, its adoption can help the organisation define a path to information security and data protection consistent with the regulations, reducing the necessary costs and increasing the effectiveness of the implemented measures.

Introduction

The diffusion of information systems within companies implies a double outcome: while on the one hand many of the decisional and productive processes are optimized, thanks to the work of personal computers, on the other hand, entrusting computers with the storage and management of data vital to an organisation, puts the company at risk of any attacks by malicious people. These malfunctions could lead to a slowdown or closure of production and decision-making processes managed by the computer system.

To avoid these risks is necessary to carefully study the causes, analyse the possible behaviour of those who try to attack company's Information Systems, not just information stored or processed in IT systems, and prepare appropriate countermeasures that can neutralise or minimise the danger of attacks or at least their consequences. (Shaqiri, 2014)

In order to protect data assets and to maintain Information Security companies must improve behaviour and culture within all its employees. One way to do so is to apply on-going awareness activities and to adhere to International Security Standards.
Moreover, it certainly cannot be surprising that even governments around the world have now placed cybersecurity as a priority topic within their political agenda. From the comparative analysis of currently public cyber strategies, it can be deduced how one of the strategic pillars shared at international level is precisely the one aimed at increasing the levels of security, reliability and resilience of networks and Information Systems. This is due, above all, because in the majority of these countries the protection of information systems critical for national security (such as those assigned to the supply of electricity, telecommunications, transport, financial systems) is delegated and managed directly by private subjects and not by governments.

The protection of confidentiality cannot or does not prescind from the security criteria of the computer data itself that must be safe, that is protected by effective security measures and able to guarantee the achievement of the following objectives:

1. Confidentiality of Information

Confidentiality consists of limiting access to information and resources only to authorised persons and applies both to archiving and to the communication of information. Preventing a user from obtaining information that he or she is not authorised to know

2. Integrity of Information

It is the degree of correctness, consistency and reliability of information and also the degree of completeness, coherence and functioning of IT resources. It is, therefore, necessary to prevent the direct or indirect alteration of information by:

- Unauthorised users or processes that can delete or damage data
- Accidental events (e.g. if the server is placed under the air conditioner and this loses water)

3. Availability of Information

Availability is the degree to which information and computer resources are accessible to users who are entitled to them when they are needed.
It must be assured in an uninterrupted manner by resorting to the adoption of a plan that ensures continuity of services, also called Business Continuity Plan. (Chia, 2012)

The management of this new risk, cyber risk, requires resources, and many.
If on the one hand, it is true that the various security systems and software are needed, it is also true that they are not enough.
It takes management processes, training programs, safety culture, awareness. We live in a world that is not designed to keep in mind safety, neglecting prevention and resolve problems when they occur.
Unfortunately, security has a certain cost, in the face of such a potential risk but that if it hits it can wipe out a small medium-sized company. It is this lack of awareness that leads, especially the administrators of SMEs, the owners, to not invest enough on computer security. It’s definitely time to wake up and invest way more in security than ever before as cyber threats are getting worse and worse by the hour, if not minutes.

Unfortunately, security has a specific cost, in the face of such a potential risk but that if it hits, it can wipe out a small, medium-sized company. It is this lack of awareness that leads, especially the administrators of SMEs, the owners, to not invest enough on computer security. It is time to wake up and invest way more in Security than ever before as cyber threats are getting worse and worse by the hour, if not minutes.

Assumptions

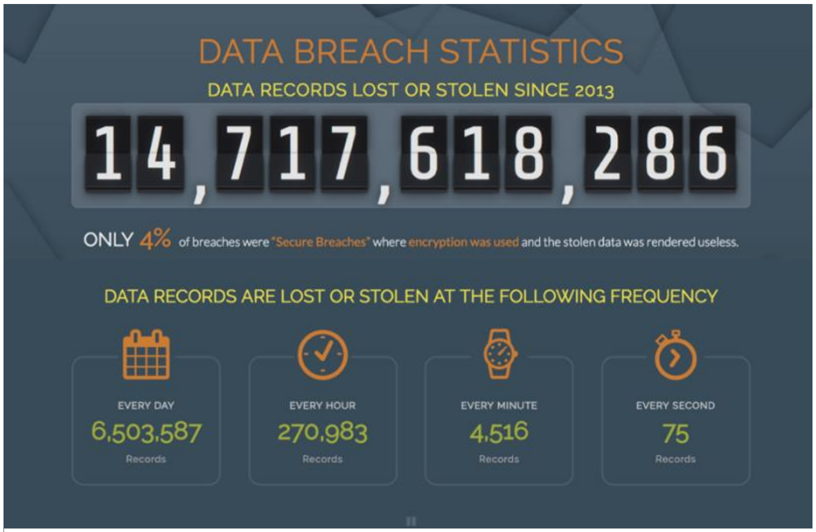

DATA BREACH STATISTICS
DATA RECORDS LOST OR STOLEN SINCE 2013
14,717,618,286
ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.
DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY
EVERY DAY
6,503,587
Records
EVERY HOUR
270,983
Records
EVERY MINUTE
4,516
Records
EVERY SECOND
75
Records

Figure 1 Source https://breachlevelindex.com/

Information is the bread and butter of the Travel Industry; effective use of technology is fundamental to the tourism sector. ITs have undoubtedly become one of the essential elements of the tourism industry as in few other economic· activities are the generation, gathering, processing, application and communication of information as necessary for day-to-day operations. The rapid development of both tourism supply and demand makes ITs an imperative partner of the industry, especially for the marketing, distribution, promotion and coordination of the industry. The reengineering of these processes is particularly evident in the tourism product distribution, where a paradigm-shift is conspicuously experienced altering best practices and introducing new players (Buhalis 1995; Wayne 1995; Poon 1993; Sheldon 1994 and 1997). For the aspects mentioned above, it is of paramount importance for any respectful travel organisation to implement a stable Information Security Management System and to adhere to at least one international security Standard Framework. For an international travel consultant agency, the risks are multiple: cyber-attacks can subtract tour ideas but also list of customers, personal data (incurring in this case in criminal trials because of the privacy laws), payroll, business plan, list of suppliers, cash data, bank details, credit card details and the list does not end here.

As the research is related to Bespoke International Tour Ltd (further on in this document also indicated merely as a Company), based in London, we can affirm the travel consultant agency is subject to the United Kingdom jurisdiction and, until remains in the E.U., the GDPR Regulations.

The Company acts as an intermediary between the customers and local franchisee. The NAS (Network-Attached Storage) and its Data Centre reside in the United Kingdom.

All customers must register with the Company and have a verified profile, address and telephone number, and preferably supply a government ID. The users can edit their profile, buy tours or directly book an excursion via the Company app or website. The user can review the services received and can be reviewed. In the event, the user wants to delete its profile and *all* the information stored with it he has the right to do so.

Threats

According to a security expert, the travel industry staff are the "weakest link" in the fight against cybercrime. Cyber consultant Bruce Wynn said cybercrime attacks risked bringing down entire businesses. He was speaking at the launch of anti-fraud group Profit's Secure Our Systems campaign, backed by Travel Weekly. There was a 92% rise in the number of cyberattack reports made to Action Fraud between January 2016 and September 2018, from 1,140 to 2,190, according to the City of London Police's National Fraud Intelligence Bureau. Reports of hacking, in which fraudsters gain unauthorised access to data, saw the most significant increase, up 110%.

Wynn believes all travel firms will have experienced cyber attacks, but some may not know it. (Dennis, 2018).

To add insult to injury, a new report by Dashlane found that 89% of travel sites leave their users' accounts perilously exposed to hackers due to unsafe password practices.

The *Travel Website Password Power Rankings* found that only 11% (6/55) passed with a score of 4/5 or better, and only one travel-related website received a perfect 5/5 score: Airbnb.

Unlike Airbnb, other household names, American Airlines and Carnival Cruise Lines failed, receiving a score of 1/5. The websites even allowed Dashlane researchers to set up accounts with alphanumeric passwords "12345" and "password." (Security Magazine, 2018).

The hospitality and travel industries have attracted some of the most significant cybercrime incidents in the last few years, and there are several reasons for this. The sector deals with billions of transactions that use rich customer data and rely on many layers of third-party vendor technologies. This is a system ripe for sophisticated hackers to exploit.

When Starwood Hotels and Resorts reported that its guest database of 500 million customers was stolen, it was unbelievable by the scale of the breach. However, perhaps the most unexpected news is that while this "unauthorised access" was discovered in early September of 2018, it can be traced back to 2014.

In 2015 Starwood had to notify customers of another massive data compromise. There are no reports *yet* that link these two events, but it does beg the question – "How was this missed?" While the specifics around this latest incident have not been publicly disclosed, Starwood has confirmed that stolen information for approximately 327 million guests includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. (SecureLink, 2014)

International tour intermediaries rely heavily on multiple suppliers and its network of local agents to sell their services. This requires a complex centralised system and security management, unparalleled in other industries. For this reason, it is crucial to implement a supplier access oversight procedure as statistics point to 63% of data breaches involve third party vendors. (SecureLink, 2014)

What are cyber threats?

A modern computer system has millions of lines of codes, each of these software elements, unfortunately, has some defects, especially once features are added without being adequately tested for malicious activity.

These defects or flaws when implemented to gain access to areas they were never meant to or use software features in ways they were never intended are known as vulnerabilities. (Nick Ioannou, 2019)

Here are some of the most dangerous threats, together with their vulnerabilities, and countermeasures:

INTERNAL ATTACKS

Entrepreneurs and CEOs are continually warned about cyber attacks coming "from outside", but those are not the only ones they should worry about. Hackers can hide even within the same organisation.

The occurrence of cyber attacks by employees or suppliers with very close links with the company is now widespread. Internal computer threats are genuine and growing. Now, we can also be sure that we have the most honest employees in the world, but criminal behaviour is not the only one that causes data breaches. (Zadelhoff, 2016)

What represents the most significant threat in the case of internal violations is negligence.

A recent survey conducted by Forrester Research, entitled "Understanding the state of data security and privacy", (Heidi Shey, 2016) revealed some interesting information on internal IT security measures:

25% of survey respondents believe there is an internal hacker at the origin of data breaches in the last two years (from the survey date).

Participants also stressed that employee negligence caused:

36% of violations.
42% of participants received safety training
57% did not know the company's security protocols.

This teaches that an entrepreneur should never lower his guard and think he is safe.

Even the negligent employees at the federal level caused losses of sensitive data, according to a report by MeriTalk (MeriTalk, 2015). Moreover, always according to this report:

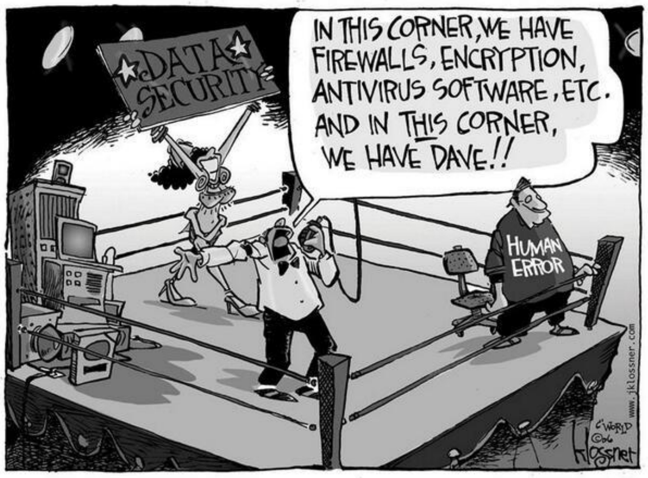

DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©WORLD ©06
KLOSSNER

Figure 2 posted on Mar 03, 2009 (KLOSSNER, s.d.)

66% of survey respondents believe that IT security is time-consuming and too restrictive
60% have blamed IT security measures on their work for various slowdowns in the workflow
31% said they ignore these measures at least once a week
20% said that security measures interfere with job completion

It is often difficult to protect oneself from hacker attacks because, in order to prevent a system violation, the processes and systems that have to work together synergistically are many.

Vulnerabilities must be identified by all significant business departments that collaborate. This includes, by way of example, IT, administration, frontline employees and third parties working on site.

Another critical factor is to implement a company culture!

A company is not just profit but above all the ability to develop tangible and intangible resources to achieve a goal and not just a financial one. It is culture, and it is creativity, it is a future to be built together, above all in respect for every employee's dignity and social ethics. Women and men, who are the protagonists of the company, with their dreams, their professional abilities, their commitment, their loyalty, build the company and transform it every day into a productive reality of tangible and intangible assets through their creative activities. These facts are vital to sustaining Security in the organisation.

Even more so today, at a time when finance and technology are likely to turn people into robots and robots into people. (KLOSSNER, s.d.)

Business Vulnerability

Human Factor - The new frontier of cyber-attacks does not only target servers, critical infrastructures or computer software vulnerabilities. Cybercrime is going further. Hackers are working more and more to try to exploit people and their weaknesses for money and data theft for financial purposes, espionage activities and to establish the basis for future attacks. (Proofpoint®, 2018)

Errors and lapses in judgment - The psychological and human dimension is cited as a significant cause of safety-related accidents in different domains, and not only in the IT field. The human factor in terms of error is implicated in the medical field, in airplanes accidents or in banking transactions [see (Reason, 1990), (Kraemer, 2009)and (Liginlal, 2009)for a review], as it has been known for some time as the human factor is implicated in 80-90% of organisational accidents (Reason, 1997)

Within the CIS, human error is identified as the most frequent cause of data security problems and information concerning organisations, determining 65% of computer security incidents in this area (Reason, 1997; Lewis, 2003).

For organizations the repercussions due to human errors are many and can be expressed in terms of productive inefficiencies, loss of money and customers, origin of vulnerability to external attacks, legal causes and last but not least from an economic point of view, the public embarrassment [see (Wood, 1993), (Lewis, 2003)).

Disgruntled workers - According to Marcus Roger, one of the first authors to apply psychological analysis to Digital Forensics focusing in particular on the motivational aspect, the internals represent the category of attackers that produce the highest economic damage compared to any other type of hacker. This is due precisely to their particular position within an organisation. The motivation that best expresses what moves the work of the internals is, according to the author, revenge:

The attacks carried out by this category are often linked by the perception of an offence suffered by the organisation for which they work, by an unfair economic treatment or, at the extreme, in response to a dismissal. It is interesting to note that, based on the representation that these attackers have of the environment in which they work and the relationship that links them to the organisation, the outcome of the behaviours associated with the attack is perceived by them as profoundly justified. This justification is constituted starting from a mixture of rational and emotional motivations that have as their common denominator the reaction to an injustice suffered and a vengeful intent. (Rogers, 2006)

Countermeasures

- The staff is adequately sensitised and trained on the risks of cybersecurity and on the practices to be adopted for the safe use of company tools (e.g. recognising e-mail attachments, using only authorised software). The senior management is responsible for preparing for all company personnel the training necessary to provide at least the basic safety concepts. (SECUREWORKS, 2018)
- Turning staff into a reliable security resource requires not only training and awareness but creating a "human firewall. To achieve this level, the company has to follow five basic steps:
  1. identify the objectives: identifying any external requirements,
  2. ascertaining the gaps and vulnerabilities that require control,
  3. identifying and quantifying risks,
  4. classifying and appropriately addressing the internal roles that have different security needs,
  5. establishing success criteria;
  - Address the challenges of accidental disclosure of sensitive information due to errors and lapses in judgment; (CERT Insider Threat Center, 2013)
  - Obtain approved programs: developing a reference business case, involving and informing the workforce and focusing on the "human firewall", including a clear description of the risks that they intend to reduce;
  - Mobilise a team of experts: choosing at least one communication expert, looking for internal experts, carefully choosing external help, using a *personal touch* and making the content readable;
  - Monitor the program: celebrating even moderate gains, and not only radical changes, sharing with all the work team the success achieved;
  - Reward those who report the security problems of the company (bug bounty programs) confidentially by committing to resolve the bug as quickly as possible;

- Including the provision of mechanisms for anonymously reporting suspicious workplace behaviour.
- Implement a feedback loop: reinforcing weak areas, ensuring that their content is up to date and accurate, maintaining control of its business and organisational security position.
- In this historical moment, marked by the advent of EU Regulation number 2016/679 on the protection of personal data, more than ever it is vital that every company begins to (re) evaluate its management of information security.
- Cultivating a culture of trust
- Senior management must set a tone that reverberates from the "control-suite" to the "shop floor".
- Six essential rules to protect sensitive data:
  1. Know what data to protect, where it is and who is responsible for creating and maintaining a data record;
  2. Create a list of employees who have access to sensitive data, minimising privileges ALWAYS and granting access ONLY to the necessary ones. Particular attention should be paid to employees in the legal and accounting departments. It is of paramount importance to terminate those that are no longer in use or linked with employee no longer employed in the company.
  3. Companies must also implement software to track the activity of privileged accounts. By doing so, it would be easier to allow for a swift response if malicious activity from an account is detected before the dealing of the damage. (How to Stop DDoS, 2018)
  4. Carry out risk analysis in order to identify potential risks to the organisation's data, thus reducing the risk of having to deal with a far more expensive infringement;
  5. Install reliable security software and perform regular scans to minimise the threat of data loss at the hands of cybercriminals;
  6. Regularly backing up the most critical and sensitive data according and storing in a different location;
- Analysis of the various types of technologies that can be used for safety, as well as an analysis of costs and benefits.
- Find out what company's weaknesses are from an external hacker's point of view. Then perform penetration tests and work on the vulnerabilities.
- Use tools to collect passwords only if employees are required to access multiple sites.
- Multi-factor authentication should be essential for access to all systems at risk.
- Encryption must be used at the system level on and off premise.
- Device recognition is critical. Knowing which devices work on the network and how secure they are is another level of protection.
- Transparency is a must, to ensure efficient operations.
- Those responsible for implementing cybersecurity must fully explain why and how the various requirements or restrictions affect the company and its employees.
- The level of protection for the different types of data should be clarified and put on paper to allow proper identification of the risk. All data is relevant, but sensitive data is more sensitive and can cause actual damage if it is violated.
- Access to protected facilities or systems must be checked and blocked if authorised employees are off-site.
- There should also be an alarm for all suspicious movements. Today's security technologies have a lot of bells and reminders to warn of the various problems that arise even during the day. However, precisely because of their almost constant presence, the user can start ignoring them totally or otherwise not paying attention to them. It is therefore essential that employees be trained on recognising the different types of alarms.
- An efficient system of electronic and paper data disposal should be set up and also for devices that are no longer in use. Destroy, destroy, destroy.

- Managers should be encouraged to be alert to employees who have negative thoughts about the company or their work;
- Prepare a centralised system for collecting, storing and analysing real-time log files, both those generated by computer systems and those originating from network activities (files to be kept for at least six months). (Walker-Roberts & Hammoudeh, 2018)

SQL INJECTION

The security of a website is not only guaranteed by a well-configured web server, or by an SSL tunnel but must be implemented conscientiously, even by those who develop the web application. One of the most classic types of attack related to the web, widespread but often underestimated, is to hit the heart of the web application, i.e. the database: it is the attack of SQL injection type. SQL injection means exploiting a vulnerability in relational databases, which uses the SQL language for data entry. It is essential to keep in mind that this phenomenon can affect any programming language and any DBMS.

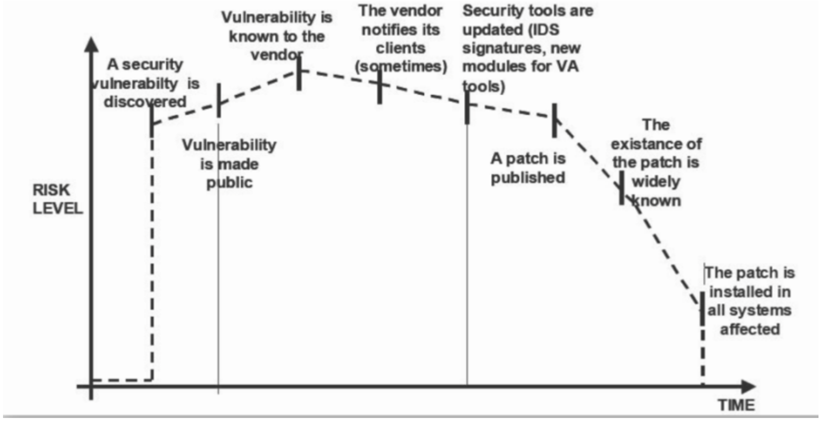


Figure 3 Window of Vulnerability (OWASP, 2016)

Business Vulnerability

- Web Applications/
- Database Management System
- User input
- Programmer distraction
- Incorrect implementation
- Cookies

In principle, every site and web application risks being subjected to SQL injection, as long as SQL is the language used for the database; in fact, too often the developers of the programs that communicate with the database do not deal sufficiently with the security aspect. Discovered vulnerabilities do not remain secret in the vast World Wide Web for long, and there are therefore pages that inform about current vulnerabilities and also reveal to cybercriminals how they can find sites affected by these vulnerabilities by doing a Google search.

Thanks to standard error messages, it gets quickly checked whether the results can become a potential target for hackers.

User input can be transmitted in various ways: through URL (query string), through an HTML form or a custom-built cookie. The hacker takes advantage of these inputs in the database interface that are not correctly filtered and where there are metacharacters such as double dash, quotes, quote elements and semicolons. These characters have special functions for the SQL interpreter and allow the external modification of the executed commands. Often a SQL injection is related to programs in PHP and ASP that have old interfaces. Here, at times, the inputs are not filtered the right way and therefore represent the perfect target for a hacker attack.

With a targeted use of function characters, an unauthorised user injects other SQL commands in this way and manipulates the records so that they can be modified, read or deleted. In severe cases, it is even possible that by exploiting this method, the hacker manages to have access to the system command line and thus reaches the entire database server.

A particular type of SQL injection is CRLF injection (also called Cookie Tampering), which in other words is a technique of SQL injection, where arbitrary code is inserted into cookies.

Here, then, the need to implement a series of preventive checks in order to stem any possible flaw of their web applications. Vulnerabilities can be numerous (depending on the attacker's imagination) and usually derive from a distraction of the programmer or an incorrect implementation.
Since vulnerable databases are detected quickly and SQL injection attacks are performed just as easily, this method is one of the world's favourites. So cybercriminals act by implementing different attack patterns and exploit to their advantage the recent vulnerabilities of the applications involved in the process of data management, targeting primarily the most popular ones. (Veracode, 2019)

Countermeasures

- Verify and filter the methods and parameters that use linked applications to insert inputs into the database. Data should always be present in the classic file types for a database. If a numeric parameter is requested, one can, for example, check it with a PHP script including the is_numeric() function. In the case of filtering, it means that the relative special characters will be ignored.
- We must ensure that applications do not show visible error messages, that reveal information about the system used or the database structures.
- The so-called prepared statements, which can be used with many DBMSs, have now become common. These predefined instructions were initially being used to perform frequently asked queries and, due to their structure, also reduce the risk of SQL injection. The parameterised instructions communicate to the database the actual SQL command separated from the parameters. Only the DBMS itself at the end combines both and automatically filters the decisive special characters.
- The server security, on which DBMS is executed, obviously plays a vital role in the prevention of SQL injections. First of all, the operating system must be strengthened according to the known scheme:
- Install or activate only applications and services that are important for database operation.
- Delete all user accounts that we do not need.
- Make sure that all relevant system and program updates are installed.
- The more requirements that are attached to the security of the site, the more we should consider the use of Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS). These work on the server with different recognition systems to detect attacks promptly, issue the similar warnings and also automatically activate, in the case of IPS, the right countermeasures. An application-level gateway can also be a useful preventive measure, a firewall component that controls data traffic between applications and the browser directly at the application level.
- Like our operating system, the database should be cleaned of all those irrelevant factors and updated regularly. To do this, we must delete all stored procedures that are not needed and turn them all off.
- Unnecessary services and user accounts. We need to set up a database account, to be used only for web access and with minimum permissions. It is also advisable to save all sensitive data in our database, such as passwords, in an encrypted form.
- As for prepared statements, it is strongly recommended not to use the PHP MySQL module and to choose MySQLI or PDO (PHP Data Objects) instead. (Huang, et al., 2017)

CROSS SITE SCRIPTING (XSS)

The widespread use of dynamic content sites that use server-side languages (such as ASP and PHP) has favoured the development of particular hacking techniques, designed to affect users of web applications. One of the best known is undoubtedly the Cross-Site Scripting (XSS), a popular type of threat which consists in an attacker inserting a malicious code (JavaScript) into the browsers using a vulnerable web application.

Business Vulnerability

- Web browsers

- Web applications
- Insufficient input control in the form

Attackers can enter a malicious code in different ways. They might convince the user to click on a link (Reflected XSS) or wait for the user to visit a page that already contains the malicious code inside it (Stored or Persistent XSS), which allows an attacker to insert arbitrary code as an input of a web application, so as to modify its behaviour to pursue its illicit ends. If a script allows this type of attack, it is easy to build an ad hoc URL and send it to the user who will be the victim of the subterfuge. The user, unaware of this change, will seem to use the standard service offered by the vulnerable website. Web pages or email are the ideal means to carry out the attack.

Let us consider an example. We know that when we use a service that requires the entry of a username and password, often this data is recorded on the user's machine in the form of cookies. For obvious security reasons, the data contained in the cookie can only be accessed by the website that created it but let us suppose that the site in question uses an application that is vulnerable to XSS: the attacker can inject a simple JavaScript that reads the cookie from the user and reports it. The user's browser will allow reading because the JavaScript is executed by a site authorised to read the cookie! The immediate result is that the attacker will have access to the cookie and, depending on the information contained, he will be able, for example, to read the user's mail, or to use his nickname in the forum he is attending, and so on.

It should also be noted that Cross Site Scripting usually requires an active intervention by the victim in order to function; even clicking on a link in a web page or an e-mail message can hide pitfalls of this type. It is important to remember that SSL encrypted connections do not offer adequate protection for these flaws.

In general, any web application can be at risk if it does not implement appropriate controls on user input. However, bugs found in web applications are usually resolved in a short time, and patches are integrated into later versions of the scripts. (OWASP, 2018)

Countermeasures

- The input of the search field could be analysed to correct or delete any codes.
- The web server could:
  - Be set to redirect invalid requests.
  - Detect simultaneous access and invalidate sessions.
  - Detect simultaneous access from two different IP addresses and invalidate sessions.
- The website may only display the last digits of the credit card used previously.
- The website may require users to re-enter their password before changing the registration information. (Wikipedia.org, 2019)
- Users could be instructed not to click innocent-looking links which are in reality malicious
- Secure input handling needed either through:
- Encoding, which escapes the user input so that the browser interprets it only as data, not as code.

Validation, which filters the user input so that the browser interprets it as code without malicious commands. (Valbuena, 2016)

PHARMING

Pharming acts either by attacking the server or attacking the client, making the defence much more complicated. The hackers act both on DNS servers and the end user.

Business Vulnerability

- DNS servers

The "local" pharming redirects the user from legitimate websites to fake sites, using the attack via the DNS cache. The part of the system that determines which website is present at a given address is changed before the Internet search starts. The affected user enters the correct URL but ends up on a site whose IP is false.

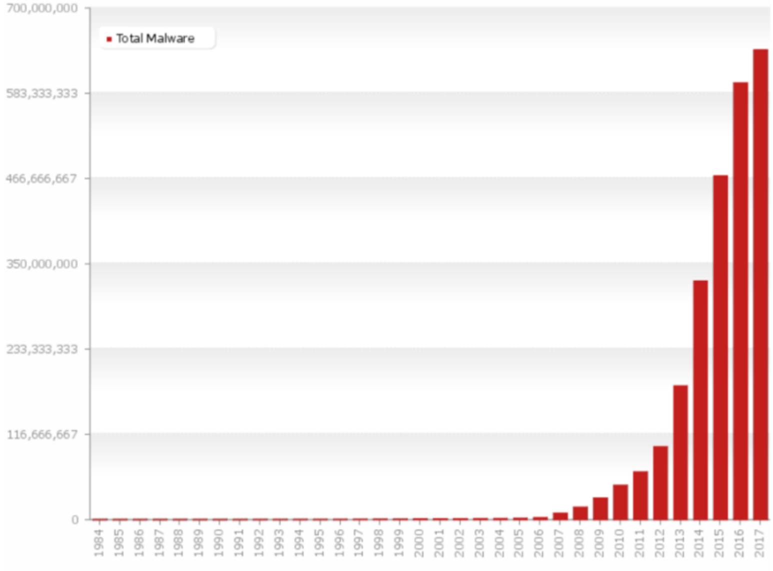
The ultimate goal of pharming is the same as phishing that is targeting a victim to a web server "clone" equipped to steal the victim's data.
Pharming is particularly insidious because, in case of a DNS server violation, even users with fully protected and malware-free devices can be attacked.

Countermeasures

- Firewall
- Updated Antivirus
- To defend against pharming, it may be useful to put the file C: \ WINDOWS \ system32 \ drivers \ etc\hosts read-only, use secure DNS servers and disable DNS cache if possible.
- If the site we connect to is a secure site before access, we will be shown a *digital certificate* issued by a known certification authority, which will report the exact site data. It is crucial to read it carefully.
- We must always check that the URL of the site we are visiting is written correctly.
- We must always check that the URL is changed to "https". The "s" stands for "secure" and indicates that it is a secure website.
- Using a reliable ISP (Internet Service Provider) and pay attention to the sites we visit.

MALWARE

According to the antivirus company McAfee Labs they have seen over 478 new malware threats every minute, which works out to a very scary average of 8 per second. They also recently reported over 63 million malicious URL hyperlinks and over 66 million malicious IP web addresses. So, what is malware? Any program created for damaging an operating system, compromising the functions of a computer, or making unlawful actions with a computer, data, connections (such as stealing personal data or sending emails from our email) is considered malware.
Here below is a list of some of the most dangerous ones:



Last update: 06-03-2017 20:12 Copyright © AV-TEST GmbH, www.av-test.org

Figure 4Wordwide evolution of malware

Viruses – A virus is a computer program composed of a series of simple instructions, like any other program. It is usually composed of a minimal number of instructions and is specialized to perform only a few simple operations and optimized to use the smallest number of resources, in order to make itself as invisible as possible; it was written to "embed", and that is to be confused with the instructions of other programs by modifying them. The main feature of a virus is to replicate and then spread to the computer every time an infected file is opened.
In analogy with a biological virus, a virus is not a self-executable program, but to be activated it must infect a host program, or a sequence of code that is automatically launched, such as viruses that exploit the "boot sector" which is performed each time the machine is started. (Pfleeger, 2003)
The technique usually used by viruses is to infect executable files. The virus inserts a copy of itself in the file with the extension ".exe" that it must infect, placing among the first instructions a jump instruction to the first line of its copy and at the end of it another jump at the beginning of the execution of the original program. In this way, when a user launches an infected program, the execution of the program is assured: the user in this way does not realise that the virus is running and is carrying out, without his knowledge, the operations contained in its code and for which it was designed.

The virus, in addition to self-replication, can carry out a series of extremely damaging operations, ranging from merely making messages appear (for example unsolicited banners or pop-ups), to opening backdoors that can allow malicious external users to access to the machine, to the capture of data and information present on the machine, to their compromise, up to their destruction.

There are some signs of recognising a virus such as when Internet connection may be slow, or absent or else Antivirus or firewall protection may be absent or disabled.

Virus-infected computers are even able to act independently, performing actions without the victim's knowledge. After a pre-established time, necessary to carry out the "replication", the virus begins to perform the action which it was written for, which may consist, for example, in destroying data or programs present on magnetic support or, simply, in making a message appear on the screen. (Symantec Corporation, 2019)

Here are the most dangerous types of viruses among those currently known:

Macro Viruses

They are the most recent and currently the most widespread, often very dangerous.

They only infect data files, so not the programs. To be precise, only document files that can contain so-called macro definitions. These are sequences of instructions written with programs such as Visual Basic and intended to be loaded and used with the Office suite applications (Word, Excel, PowerPoint and Access) and all compatible programs. The macros are used to automate certain operations in the documents, such as requesting the entry of fields in a previously prepared form. In reality, operations that can be performed using macros can also include deleting and modifying files, accessing sensitive system data, and much more, to potentially generate specific virus programs of other types. Macro viruses are relatively easier to make than previous types, so there are many. Moreover, if correctly created, they can be portable and therefore also work on various operating systems, i.e. with all those that have suites of programs that can read the same file and then run macro-definitions (such as Macintosh). For this reason, we must always be suspicious if a downloaded document asks us to activate the macros.

Memory Resident Viruses

These types of viruses use the RAM as attack tool and they "live" inside of it. Infections caused by in-memory attacks are not persistent, and a reboot of the PC would lead to disinfection. The attacker is often not interested in maintaining persistence, for two reasons:

a compromised system is not patched and will probably not be for a short while, so re-infection is extremely simple;

critical systems, the most interesting ones, are rarely restarted, making the time of persistence sufficient to achieve the hackers' goals.

Overwrite Viruses

These types of viruses delete any information in a file they infect with apparent problems of execution.

Direct Action Viruses

These viruses attack once they are executed. They will infect the files in the directory, or the folder specified in the AUTOEXEC.BAT. These viruses can be found in the HD's root directory, although they keep on moving location. (TYPES LIST, 2019)

FAT Viruses

This type of virus modifies the FAT (File Allocation Table) of the system. The FAT contains the index of the names and addresses of the files. The virus modifies it to run before the original program.

They are usually located in the disk but affect the entire directory.

Web Scripting Virus

Many websites today are web applications; real programs run on our browser.

Viewing online videos, for example, requires the execution of a specific code that loads the player. Some sites automatically start malicious scripts that, even if they are not blocked in time, cause substantial damages.
Usually, a warning pop up appears, an authorisation request or a message ("your computer is infected, do you want to scan now? OK").
In these cases, we must close everything and not accept anything that comes from an unknown site.

Multipartite Virus

They are among the most complex and one of the most dangerous viruses. They can infect both boot sectors of disks (such as boot sector viruses) and programs (such as file viruses). The classic behaviour is that even if we delete the virus from infected files, remaining active even in the boot sector will re-infect as soon as possible (as a rule, at the next boot) such files. The argument also goes to the contrary: by eliminating the virus from the boot sector, but by launching one of the infected files, the virus will also re-populate again in the boot sector of the system disk.

Companion Viruses

Instead of modifying an existing file, it creates a new one (usually a *.com* one because it has priority status concerning the *.exe*) which, once called the file from the prompt, is executed instead of the original program. At the output, this then executes the original program to make things appear completely normal. A simple verification of the integrity of the files does not give, in this case, any alarm.

Polymorphic Virus

These are viruses that can change over time to avoid being deleted from our computer. Lately, they are growing and are becoming more widespread. They can infect the computer and do not give any sign of their presence for months, then with time they become more powerful and begin to take possession of our machine. As if this were not enough an antivirus cannot notice the polymorphic virus, if it is in its initial phase and remains hidden.
(Types List, 2015)

Trojans - Trojans are a particular type of malware that criminals can use to take complete control of our mobile or fixed device and perform almost any type of operation: from blocking, modifying and deleting data to knock out the computer system. For example, it hides in a free program, in an attachment to an important email that we have to download on our computer, and it comes from our boss, or in video games, applications and movies. Once installed, it often acts silently, without the computer owner noticing its nature.

A Trojan virus can do almost anything. It can, for example, turn computers into a zombie that will be placed inside a botnet, i.e. a system used by malicious people to launch cyber-attacks around the world. However, it is also able to monitor any activity we perform on the device in question: from all messages written through any platform, geolocation, passing through the internet history and activation of the camera to take pictures as well as the microphone to record the environmental audio.

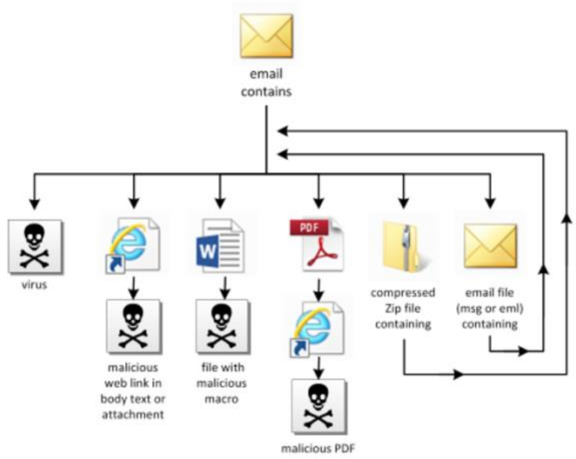


Figure 5 Threats via e-mail (Boolean Logical Ltd, 2018)

Unlike other computer viruses, Trojans have no autonomous diffusion, but must be downloaded by the user who has an active role in the propagation of the malicious program. They appear as executable files ('exe', 'vbs', 'bat', 'js' and so on), although they often mask their origin with tricks. Like to rename the file containing the trojan with different extensions, for example, "Documento.txt.exe". In this way, the attachment is not visible as ".exe" because the attacker exploits the fact that the operating systems signed by Windows do not show all extensions by default. Instead, content created in this way is displayed as "
.pdf", despite being executable, causing users to open it.

However, disabling the option of known file types is not enough: another trick used, especially in email attachments, is that of "spaces". Referring to the previous example, what would happen if we named the executable file of our virus as nameFile.jpg   .exe?

The user, even if he has disabled the option that hides the extensions of known file types, could "see" only the initial part of the name nameFile.jpg. This happens because the name may be too long to be viewed entirely in the space available, both because it is easy for our eye to stop at the characters before the spaces, ignoring the next part.

What can be done to limit this type of problem?

It is best practice never to open attachments directly from the mail program, especially if coming from unknown senders. It is always better to save the attachment on our disk (without launching it) and thus have the possibility to display its name in its entirety. This will also allow us to use our antivirus (not always integrated with the e-mail program) to analyse the file for any problems before the fatal "double-click". (Kaspersky Lab, 2019)

Worms – self-replicating malware that duplicates itself to spread to uninfected computers.

The worm is one of the most widespread malicious programs that, like the Trojan, requires the unwitting collaboration of the users. In fact, in general, the worm sneaks into computers through an attachment or executable script, contained in an e-mail message. Worms can blend into the system and antiviruses, although worms are different programs, struggle to find them. The main feature of the worm is the ability to self-replicate. The purpose of any malware is to hit as many victims as possible and the worm, if it infects the machine, accesses the e-mails and sends several copies of itself.

Moreover, without the involuntary intervention of the user, as happens with other viruses. Also, that is not all. The most sophisticated worms can be used by hackers to remove the security of the infected machine and install other malware. It is very common that they are used for the installation of backdoors in the computer protection network, or keyloggers, programs that store everything that is typed on the keyboard, allowing in fact to reconstruct all the operations performed, often using memory sticks on laptop ports.

The worm is also often used to tilt the affected machines, overloading the LAN with requests (DoS attacks). (Kaspersky Lab, 2019)

Ransomware There is different types of ransomware that cause many damages to a system.
The various types are analysed below:

Scareware

These are special malicious software that is usually aggressively sponsored as if they were utility programs to improve and optimise the system. In these cases, the user downloads the software voluntarily and installs it, convinced he had found a new program for Windows maintenance. Some scareware can promise to repair the registry or increase the speed of the operating system. The scam is realised when a series of errors and problems are found on the PC, often false ones, and the user is invited to purchase a software license to solve the problem. The user is then encouraged to buy the license, but in reality, it is just a fraudulent payment triggered by the ransomware.

Virus locks screen

This type of ransomware is very dangerous because it freezes the computer screen and we cannot use the PC. To be able to unlock the screen we have to pay the ransom; otherwise the computer remains unusable.

Fortunately, even if this virus is somewhat hostile, data recovery experts can recover files through other tools without having to pay the ransom.

- Ransomware that encrypts the files

This malware is among the most aggressive and difficult to eliminate. Unlike those seen above, the software encrypts the files on the PC but does not block the screen. The user can continue to use the computer, but the main files and documents will be inaccessible because they are encrypted. It is the ransomware that has caused more damage in recent years and is present in many more or less powerful variants. Usually, the infection is done by downloading and opening the attachment of a well-written email. There have been many companies that have lost important documents due to this malware. To decrypt the files, a ransom must be paid.

In some variations, it is possible to decrypt files by following more or less complicated guides, without having to pay the ransom. However, in some cases we could risk compromising files forever, destroying them permanently, so it is essential to contact an expert in the field to try decryption. At the moment, no expert can guarantee the recovery of encrypted data. The success of recovery depends on the variant of the virus.

There may be less aggressive variants than others, with which it is possible to decrypt documents.

As humans develop software, and humans make mistakes, to date there is no such perfect method of writing code. Therefore, practically every software contains vulnerabilities – that is, errors through which hackers can take control of an information system and compromise its data.

Business Vulnerability

- IT Systems
- Network
- Microsoft Windows OS
- Web Server Software
- Applications
- An unpatched vulnerability in an IT system
- MS SQL
- OS UNIX

Over the years, a large number of network worms have been created that can exploit vulnerabilities in IT systems and the Internet; among them, one of the best known is undoubtedly CodeRed.

CodeRed was detected, for the first time, on 17 July 2001; according to some estimates, this worm has infected a total of about 300,000 computers, effectively preventing a multitude of businesses from conducting normal business activities; in this way, it caused considerable financial damage to a large number of companies located in various countries. Although Microsoft has released, together with the Security Bulletin MS01-033, a particular patch designed to close the vulnerability used by the network mentioned above worm, some versions of CodeRed continue to spread through the Internet. The effects of the virus included Defacing which consists in illicitly changing the home page of a website (its "face") or modifying, replacing it, one or more internal pages.

Detected at the end of January 2003, it used an even simpler method to generate computer infection on computers equipped with the Windows operating system and its MS SQL server; in this case, it was the exploitation of a buffer overflow vulnerability in one of the UDP packet processing subroutines. Although the worm was relatively small in size - 376 bytes in all - and used the UDP communication protocol, which was responsible for the rapid transmission of small volumes of data, Slammer could still spread at an incredible speed. According to some estimates, the Slammer worm has infected approximately 75,000 computers worldwide in the first 15 minutes of the computer epidemic in question. (McElhearn, 2016)

Some standard installations of the MS SQL server, in fact, did not protect the "SA" system account with a special password, thus allowing anyone who had access to the system through the network to execute arbitrary commands within it. Using this exposure, the worm configures the "Guest" account in such a way as to obtain full access to the files stored in the computer; subsequently, it provides for uploading itself to the server to be infected.

Inevitably, all operating systems contain vulnerabilities and exposures, which can be targeted by hackers and virus writers, to pursue their goals. Although the vulnerabilities identified in Windows gain greater prominence and notoriety, given the enormous number of computers on which this operating system is installed, it should be noted that even the UNIX OS has its weak points.

For years, in the UNIX world, one of the most popular exhibits was the "finger" service. More precisely, it is a service that allows users who are outside a network to see who is connected, at that precise moment, to this network, or from which location the users are accessing the computer, as well as which network resources are used. The "finger" service is undoubtedly useful, but, at the same time, it can reveal - or rather "expose" - a great deal of information that can be exploited by hackers. It is recommended to disable this service. (Acunetix, 2018)

Countermeasures

- The networks and systems are protected from unauthorised access through specific tools (e.g.: firewalls and other anti-intrusion devices/software).
- All possible devices are equipped with regularly updated protection software (antivirus, antimalware).
- Using a secure host
- Daily Update Antivirus
- Always installing patches
- Control of the installation, diffusion and execution of malicious code in different parts of the company, while optimising the use of automation to allow rapid updating of defences, data collection and corrective actions. Security systems (antivirus, firewall, IPS) Use of external devices. Control of Web content, emails.
- Continuous Vulnerability Assessment & Remediation
- Daily non-authenticated vulnerability scanning program – enable all relevant firewalls to pass all IP traffic from ISP scanners.
- Periodic and predictable planning updates -reducing the amount of time in which cybercriminals have the opportunity to exploit the vulnerability.
- Avoiding programs from unknown sources.
- Not opening attachments of unsolicited mail
- Downloading apps only from official stores on mobile devices
- Employing automated systems of analysis and filtering of web content, in order to prevent the display and browsing of Internet sites that are inappropriate or potentially dangerous for the security of the systems. (Ody, 2016)

PHISHING – SPEAR PHISHING – SMISHING – VISHING

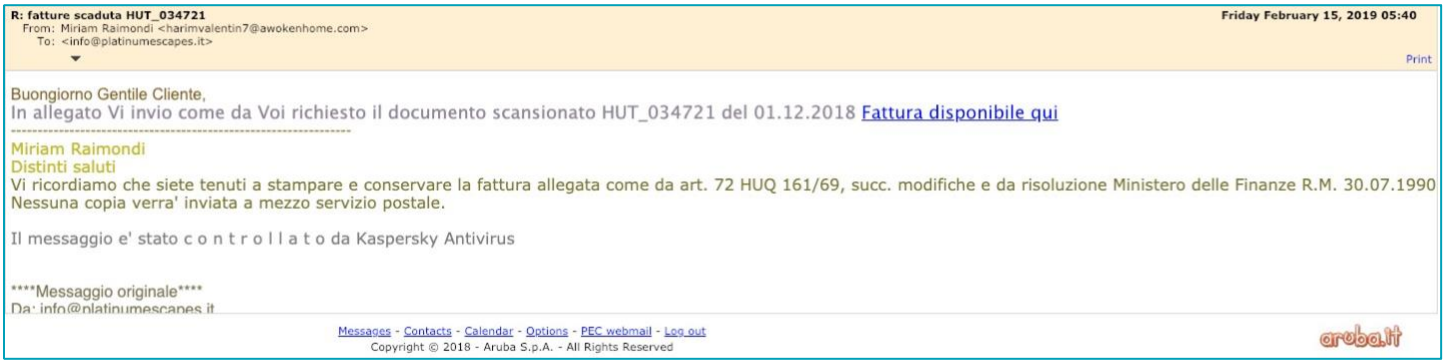
It is one of the most accessible forms of cyberattack to put into practice, but in its simplicity, it can provide a hacker with everything he needs to infiltrate every aspect of our personal and work life.

Often hackers are interested in financial data such as credit card information or the credentials of their online banking account, but also strictly personal data such as date of birth, address and ID card number. In the hands of the wrong people, this can be used to perform fraud, identity theft or purchases, as well as for the sale of information on the deep web.

According to a Symantec search, almost one in every 2,000 emails contains a phishing attempt. Anyone can be a victim: a moment of distraction is enough to believe that we are dealing with someone we trust.

Similar techniques (spear phishing) are used by hackers who could pretend to be someone within our organisation. In this case, the planning and timing activity plays a fundamental role and allows the attacker to disguise himself at best, pretending to be a customer or a supplier, and inducing the user who receives the email to perform malicious actions without realising it.

On Fig.6 we can see an email sent to a travel agency, info@platinumescapes.it. Informing the agency that an invoice has been issued and that MUST be printed and saved accordingly to the Italian law (Ministry of Finance R.M. 30.07.1990) therefore it has to be downloaded, hence the user needs to open the link.
Moreover, it mentions the message has gone through the Kaspersky Antivirus! By placing the pointer on it (Fig.7), it is likely to open a string of untrustworthy characters. The hackers hope that the victim does not control and clicks.



R: fatture scaduta HUT_034721 **Friday February 15, 2019 05:40**
From: Miriam Raimondi <harimvalentin7@awokenhome.com>
To: <info@platinumescapes.it>

Buongiorno Gentile Cliente,
In allegato Vi invio come da Voi richiesto il documento scansionato HUT_034721 del 01.12.2018 Fattura disponibile qui

Miriam Raimondi
Distinti saluti
Vi ricordiamo che siete tenuti a stampare e conservare la fattura allegata come da art. 72 HUQ 161/69, succ. modifiche e da risoluzione Ministero delle Finanze R.M. 30.07.1990
Nessuna copia verra' inviata a mezzo servizio postale.

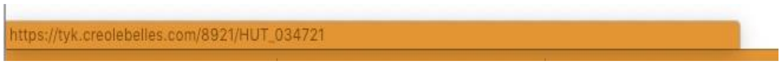
Il messaggio e' stato controllato da Kaspersky Antivirus

****Messaggio originale****
Da: info@platinumescapes.it

Copyright © 2018 - Aruba S.p.A. - All Rights Reserved

Print
Messages - Contacts - Calendar - Options - PEC webmail - Log out
aruba.it

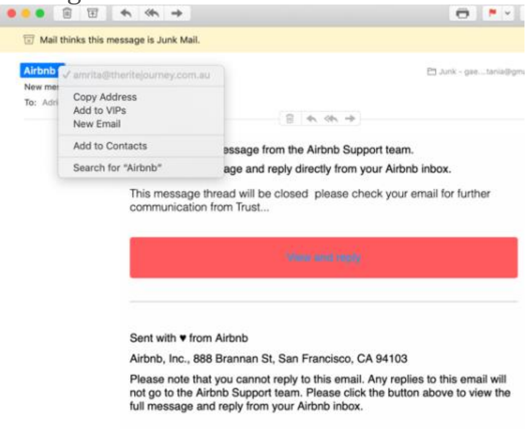
Figure 6 Malicious email 1



https://tyk.creolebelles.com/8921/HUT_034721

Figure 7 Malicious URL

On Fig.8 we can see that the sender is not from Airbnb!



Mail thinks this message is Junk Mail.

Airbnb
amrita@theritejourney.com.au

essage from the Airbnb Support team.
age and reply directly from your Airbnb inbox.

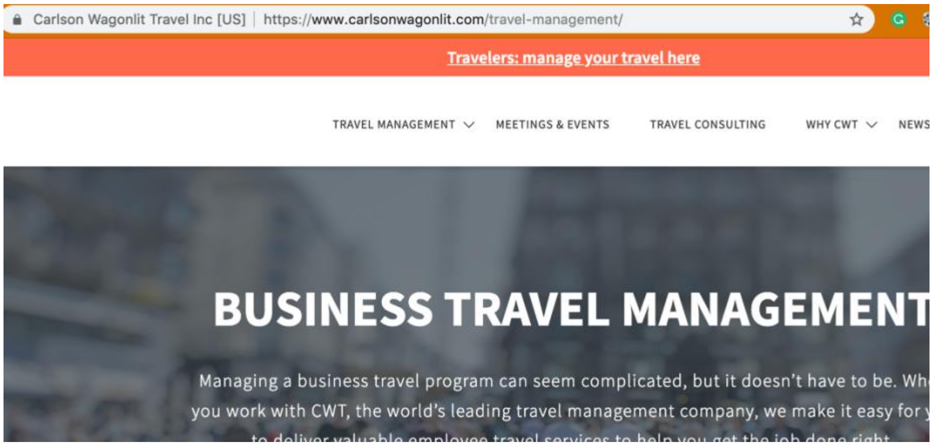
This message thread will be closed please check your email for further communication from Trust...

Sent with ♥ from Airbnb

Airbnb, Inc., 888 Brannan St, San Francisco, CA 94103

Please note that you cannot reply to this email. Any replies to this email will not go to the Airbnb Support team. Please click the button above to view the full message and reply from your Airbnb inbox.

Figure 8 Malicious email 2

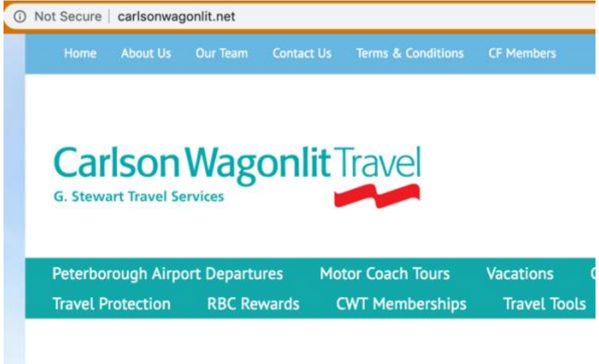


Carlson Wagonlit Travel Inc [US] | https://www.carlsonwagonlit.com/travel-management/

BUSINESS TRAVEL MANAGEMENT

Managing a business travel program can seem complicated, but it doesn't have to be. Wh
you work with CWT, the world's leading travel management company, we make it easy for y
to deliver valuable employee travel services to help you get the job done right

Figure 9 Secure site



Not Secure | carlsonwagonlit.net

Figure 10 Malicious site

SmiShing – the type of phishing attack where mobile phone users receive text messages with a website hyperlink which, if clicked on, will download a Trojan horse (malicious software) to the phone. (How to Stop DDoS, 2018)

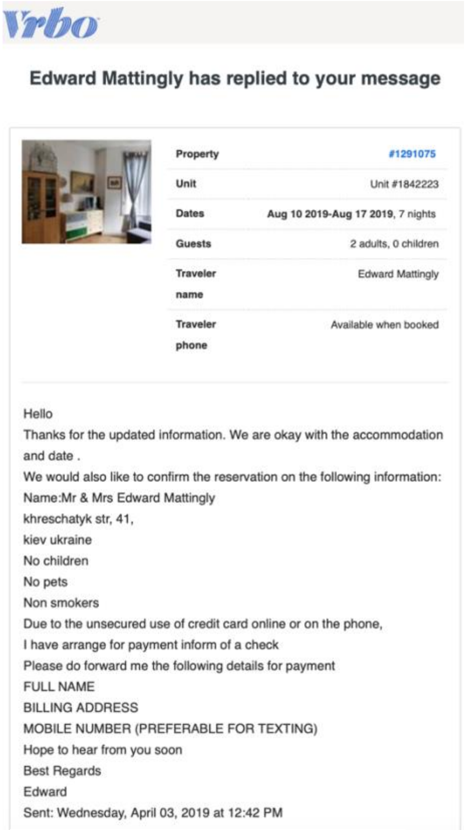
ViShing – This new electronic scam goes through the telephone instead of the Internet. The goal, however, does not change to steal sensitive data, usually banking password.

Business Vulnerability

- Not enough attention by users while reading emails
- Android (Oreo)
- Mobile password manager
- Instant Apps technology
- Password protected .zip attachments (worth noting that there are many other forms of compressed file such as .rar .arj .tar .lzh .7z and many others)
- Files ending in .zip .app .arj .bas .bat .cgi .chm .cmd .com .cpl .dll .exe .hta .inf .ini .ins .jar .js .jse .lnk .msi .ocx .pcd .pif .pl .py .reg .scr .sct .sh .shb .shs .vb .vbe .vbs .vbx .ws .wsc .wsf and .wsh.

This type of attack usually comes from a social engineering activity, aimed at exploiting the habits, behaviours and vulnerabilities of the target. While the phishing activity usually takes place through mail "campaigns" it is easier to recognise and identify (due to spelling errors, inaccurate translations or long and unclear URLs), the spear phishing activities are highly targeted, and tailor-made on the victim of the attack. Usually carried out via email messages (even if the scam has now spread also on social media, messaging services and apps), phishing tries to deceive the objective in doing what the ill-intentioned wants to do.
In practice, in a fake email, the user may get a request to reset passwords for specific accounts or change bank details so that payments go to scammers instead of the correct account. Worth mentioning is that

nowadays, with the proliferation of bots, users are asked to call a number and input sensitive data. Email is the most common way to carry out these attacks. (Digital Guardian, 2019)



Edward Mattingly has replied to your message

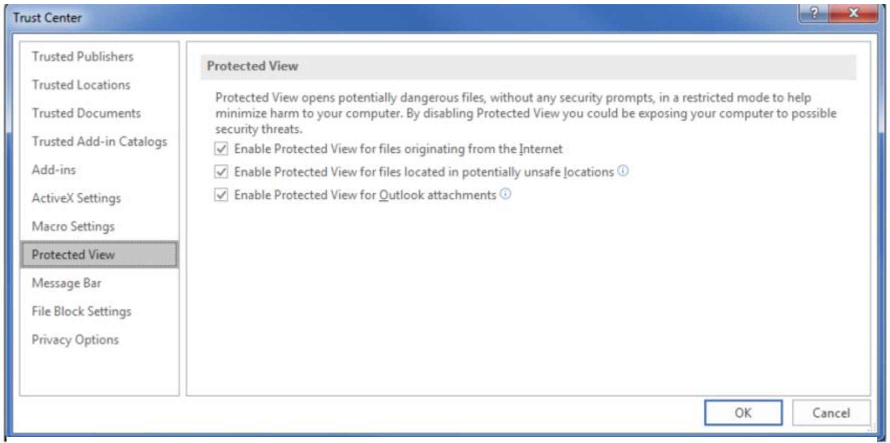
Property	#1291075
Unit	Unit #1842223
Dates	Aug 10 2019-Aug 17 2019, 7 nights
Guests	2 adults, 0 children
Traveler name	Edward Mattingly
Traveler phone	Available when booked

Hello
Thanks for the updated information. We are okay with the accommodation and date .
We would also like to confirm the reservation on the following information:
Name:Mr & Mrs Edward Mattingly
khreschatyk str, 41,
kiev ukraine
No children
No pets
Non smokers
Due to the unsecured use of credit card online or on the phone,
I have arrange for payment inform of a check
Please do forward me the following details for payment
FULL NAME
BILLING ADDRESS
MOBILE NUMBER (PREFERABLE FOR TEXTING)
Hope to hear from you soon
Best Regards
Edward
Sent: Wednesday, April 03, 2019 at 12:42 PM

Figure 11 Phishing Email

Countermeasures

- When opening an email that we do not recognise or expect, avoid clicking on the content.
- By itself, the text of an email is never dangerous. The real danger lies behind links and attachments. The latter is responsible for most of the infections in the mail. Before taking any action, it is essential to check the general appearance
- Screening the sender carefully, checking the header and the part following the @ it should correspond to the sender's website. If it is not so, it probably does not come from the company in question (Fig. 8). However, the sender's field can easily be disguised (email spoofing).
- Being wary of emails that put the user in a hurry: they seem to come from the bank, company or social network. Commonly the message is alarmistic and of the kind: "verify your account" or "reply within 48 hours".
- Paying attention to the form of the email: it must be written correctly, without grammatical errors, and must contain images in good definition.
- Paying attention to the links: just by moving the mouse over the link without clicking to check that the link is original and that It matches the official website. In general, it is good to be wary of emails containing only one line in the body with a link.



Protected View

Protected View opens potentially dangerous files, without any security prompts, in a restricted mode to help minimize harm to your computer. By disabling Protected View you could be exposing your computer to possible security threats.

☑ Enable Protected View for files originating from the Internet
☑ Enable Protected View for files located in potentially unsafe locations
☑ Enable Protected View for Outlook attachments

Figure 12 Microsoft Trust Center (Microsoft, 2019)

- When using Microsoft Office, all macros must be disabled with notification while in Protected View everything must be ticked (Fig.12).
- In case of inadvertent opening, users must be instructed not to enable Office macros;
- Checking the reliability of the site to which the email refers: if in doubt, we can check the safety on sites such as www.virustotal.com to find out if the link we are about to click on is dangerous or not.
- Paying maximum attention to attachments: usually, antivirus, safer browsers and email applications perform the necessary checks, but some malicious content is not detected. It may be useful to observe the extension of the attachment to verify that it is not double (for example, .pdf.exe).

- Employees must be instructed to NOT:
    1. use the company email for personal purposes;
    2. use the personal email on the work PC or company mobile;
    3. use simple passwords;
    4. use the same password on multiple services;
    5. share credentials with third parties;
    6. share full name, address and mobile number to an unknown source (Fig.10)
- when navigating, users must check that in the address bar there is the prefix HTTPS: // (Condition necessary but NOT SUFFICIENT for the site to be considered reliable – (SSL Strip).
  (INFOSEC, 2019)

SOCIAL ENGINEERING

No matter what a security technology business has, the investment in cutting-edge solutions could be affected by the behaviour of a single user, manipulated with a social engineering attack.

Social engineering is a fearful threat to the most protected networks. It is the most potent attack because no technology allows it to be prevented or defended. To be immune to it workers need to be trained.

Social engineering is, in general, the art of inducing people to perform specific actions by concealing the real objective of the attack. The social engineer can disguise his/her identity, pretending to be another person: in this way, through conversation or other interactions, he/she can obtain information that otherwise he/she would not get.

The consequences of a successful social engineering attack in IT are the disclosure of confidential information through deception and, in some cases, the spread of viruses or trojans.

The evolution of cybercrime in recent years highlights the tendency to jointly use advanced techniques of malware and social engineering to launch attacks increasingly sophisticated and challenging to predict or detect, such as to cause significant damage and sometimes irreparable to corporate security systems, with consequent economic losses, loss of sensitive data and strategic information, damage to reputation.

Business Vulnerability

- Outward facing roles (sales & marketing/customer service/receptionists).
- At a lower level (those who may not appreciate the importance/sensitivity of the information or site).
- Trust.
- Unwitting behaviour and people’s distractions.

Among the leading causes of companies' vulnerabilities, at the top of the ranking are the unwitting behaviour and people's distractions. It is estimated that as many as two-thirds of the attacks are not detected, the cybercriminals have become able to exploit security gaps to evade controls and hide malicious activities. More and more often malware is present in the victim's computer in a silent way and, without being detected by antivirus, they steal strategic information, sabotaging and damaging systems.

Any unsolicited advice or help should be carefully evaluated, especially if we need to click on a link, as it may very well be an attempt at social engineering. Likewise, any request to provide passwords or financial data is undoubtedly a scam, as legitimate institutions never require any password.

Also, it is imperative always to remember to check the e-mail address of any suspicious e-mail received, to make sure it is a legitimate one.

The goal is not to identify the bugs of the system to be able to hack but, as mentioned, focus on the human factor: it can also be defined as the art of digitally manipulating people so that they voluntarily surrender their data (or allow access to their IT resources).

A social engineer studies his/her victim for weeks, if not months, before being able to convince him/her that he/she is an acquaintance of his/her friend and, at that point, launch the attack.
We can distinguish two broad categories: attacks based on the interaction between human beings and attacks that exploit a computer as a means.
Among the attacks of the first category fall strategies such as impersonating someone to take advantage of the simulated role: the posing as an important person, for example, is useful in order to intimidate the interlocutor making him lower his defences; or pretending to be from technical support team can serve to steal confidential information or physically access the victim's computer.
Initially, as mentioned, the attacker must study the victim: he must find information that is useful to gain his trust and let him lower his guard. Once confidence is gained, the social engineer can put the "cards" on the table to prepare for the attack: the hacker leverages some psychological aspects of the victim, pushing him to perform the desired actions.
Authoritativeness is usually used (for example, by demonstrating expertise in a particular field such as computer security), but feelings such as fear, guilt and compassion can also be more than useful for their purposes. Other techniques that should not be underestimated, even if at first sight banaler, are the "**surfing**" (that is, peeking unobserved passwords or other information, usually positioned behind the unaware victim) or **dumpster diving** that is the recovery of material from the garbage.
The second category includes all the software-based attacks such as phishing and spear phishing, **baiting.** The baiting (literally translatable with "enticement") is instead preceded by a phase during which the social engineer creates an implicit desire in the victim, satisfied (or at least so it must appear) later thanks to the content of an email or instant messaging. For example, this can be very high discounts on smartphones and other products that have been searched for some time or confidential information that is particularly attractive or "abandoning" USB sticks or CD in order to stimulate the curiosity of the victim and scam.
(Frumento, 2018)

Countermeasures

- The passwords are different for each account, of sufficient complexity and the use of the most secure authentication systems offered by the service provider is evaluated (e.g. two-factor authentication).
- Personnel authorised to access, remote or local, and IT services have private utilities not shared with others; access is adequately protected; old accounts no longer used are deactivated.
- Education - employees should be thought about social engineering awareness and the value of the information they hold.
- Never accept anything that we are not sure about its legitimacy.
- Never accept unsolicited offers.
- Never click on links from unknown sources.
- Never provide our password or bank details.
- Software controls for employees' internet access.
- Robust filtering throughout internet gateways (Proxy, VPN).
(Olavsrud, 2010)

BYOD

The mobility offered by BYOD logics is at the same time an excellent advantage for productivity and risk for IT security.
The BYOD (Bring Your Own Device) has brought enormous benefits to businesses, thanks to the ability to work from any device in any place and time. However, all this mobility can represent a risk in cybersecurity.

Business Vulnerabilities

- Wi-Fi hotspots

- Personal devices are not part of the IT infrastructure

During a study on data protection measures, 68% of the 4,200 IT operators interviewed by Ponenom Institute and Citrix think that BYOD represents a vulnerability to information security (Ponemon Institute, 2017).

The main concern is the fact that BYOD can facilitate unauthorised access. Besides, 65% believe that the company cannot prevent employees from installing unapproved applications on devices used to work, while 48% would like a harsher practice for access to information. Then there is the question of policies and rules that are too old to be useful for security purposes, an opinion shared by 70% of the subjects.

The last aspect taken into consideration is that of the relationship between technological tools and professional skills, given that the lack of the latter often runs the risk of cancelling the expense made to improve the infrastructure.

(Kerner, 2017)

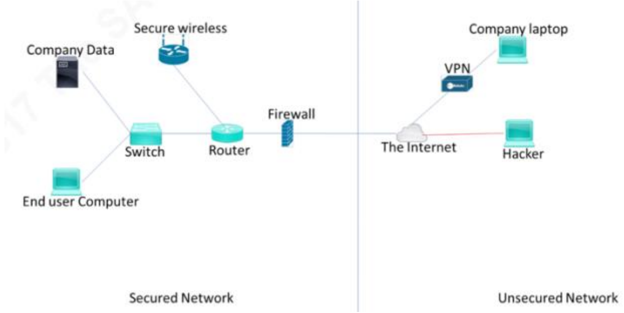


Figure 13 Typical Wired Network (Simmons, 2019)

Countermeasures

- Unified control over the digital activities of the workforce;
- Supporting a proactive line in the management of the various processes.
- Private virtual LAN: it concerns the subdivision of a physical network in many logical networks so that they do not interfere with each other; is a technique used to improve address management and the speed of traffic on the network, as well as to keep "isolated" different departments within the company.
- Use of new technologies
- Software controls for employees' internet access
- Integration of the various technologies to reduce management complexity. It is necessary to build an infrastructure that allows managing and better organise all the elements involved, to protect data not only through the security of the endpoints but also by making visible and coordinated actions possible.
- Automatic cleaning of all data, as soon as the employee declares to have lost his/her device or have suffered a theft.
- Properly training the IT department and all employees.
- Taking the right precautions could greatly help us grow our business, rather than to opt out for BYOD.
  (Kerner, 2017)

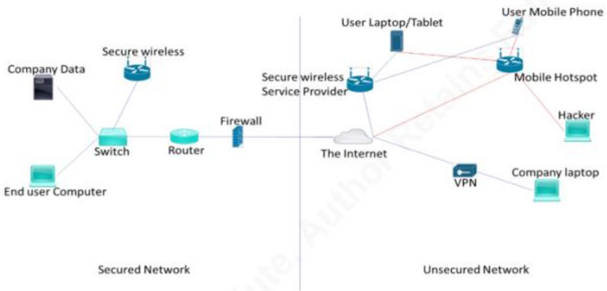


Figure 14 Typical Wired Network with mobile devices (Simmons, 2019)

DOS/DDOS ATTACK

A DoS (Denial of Service) is an attack that aims to prevent the provision or use of a service, making it unavailable or unusable to legitimate users. To increase its effectiveness and power, attackers exploit multiple machines simultaneously (for example, a botnet), thus DDoS (Distributed Denial of Service). The cyber attacker takes control of some machines, called zombies, which perform a large number of requests to the target machine, making it unavailable and thus making it impossible to .use the services provided. The same machine may be involved in both phases of the attack or become a zombie and is the final destination of the DoS. There are various methods used to take control of the machines: it can be the exploitation of known vulnerabilities or the installation of malware through a malicious link or mail.

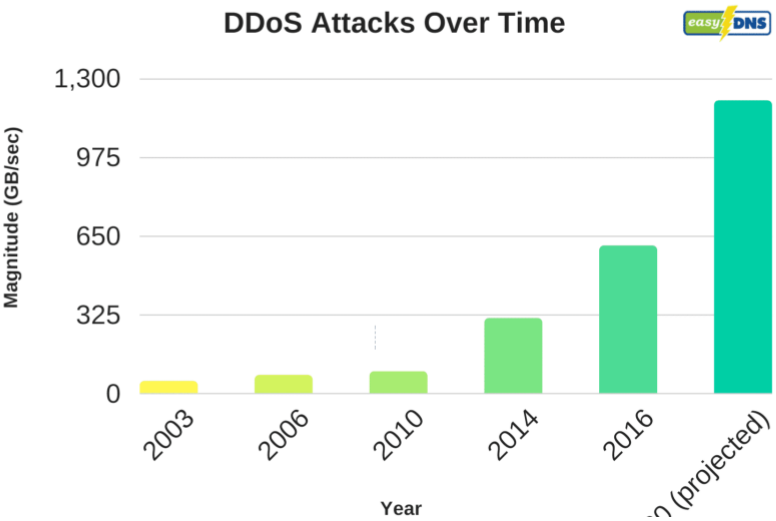


Figure 15 DDoS Attacks over time

Business Vulnerability

- Network Layer
- Applications

DDoS attacks are becoming more and more sophisticated as software piracy works diligently to weaken companies; this is why it is necessary to develop defence plans and verify them promptly. A good prevention strategy starts with knowledge. There are different types of DDoS attacks but, to rationalise methods and approaches, it is possible to make them fit into three macro-categories:

Volumetric attacks: these are attacks that aim to overcome the network infrastructure, consuming bandwidth or running out of resources.

Saturation attacks of the native state of TCP - Attackers use this method to abuse TCP and saturate not only server and firewall resources but also workload balancing.

Application Level Attacks - The goal of these attacks focuses on a single application or service at level 7.
If volumetric attacks were until recently part of the most common DDOS, today it is increasingly common to see DDOS attacks combining all three types described above; which increases not only the breadth but also the duration of the attack. (Symantec, 2019)

Countermeasures

- Deploying security audit log software
- The recognition of a DoS attack and its prevention require specific network traffic monitoring tools, capable of detecting anomalies on the traffic entering or exiting the company network, in such a way as to stop possible attack attempts. For some types are possible technical defences (syn cookies for example) or tools such as firewalls and IPS. If the attack is volumetric and directed to the bandwidth, QoS techniques are often used to try to mitigate it or make it less effective. (Symantec, 2019)

PRIORITIZING

Threats	Threat level	Business Vulnerability	Total
Internal Attacks	5	5	10
SQL Injection	3	3	6
Social Engineering	5	5	10
Cross-Site Scripting (XSS)	4	3	5
Malware	3	4	7
BYOD	3	3	6
Pharming	2	2	4
DDoS attacks	3	5	8
Phishing spear phishing smishing vishing	2	2	4

Top 5 threats:
Internal Attacks.
Social Engineering
Malware
Cross-Site Scripting
DDoS Attacks

Risk assessment measure
5 - Very Severe
4 - Severe
3 - Moderate
2 – Low
1 – Very low

Overall Risk Assessment Measure

The Overall Risk Assessment Measure unifies the two components above into a measure of risk to computer users. There are five severity threat categories, as described below.

Level 1: Very Low

Poses little threat to users. Rarely even makes headlines.

Level 2: Low

Threat type characterized either as low or moderate but reasonably harmless and containable.

Level 3: Moderate

Threat type characterized either as highly but reasonably harmless and containable or potentially dangerous and uncontainable if released into the wild.

Level 4: Severe

Dangerous threat type, difficult to contain. The latest virus definitions should be downloaded immediately and deployed.

Level 5: Very Severe

Highly dangerous threat type, very difficult to contain. All machines should download the latest virus definitions immediately and execute a scan. E-mail servers may need to come down.
(Symantec, 2018)

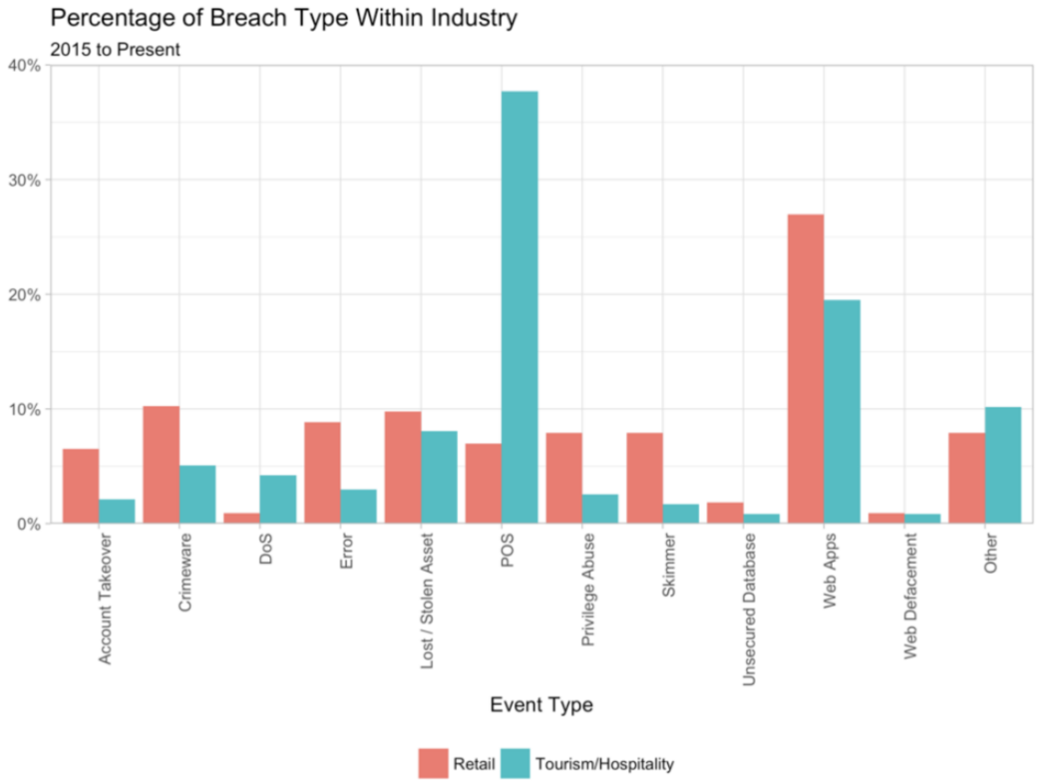
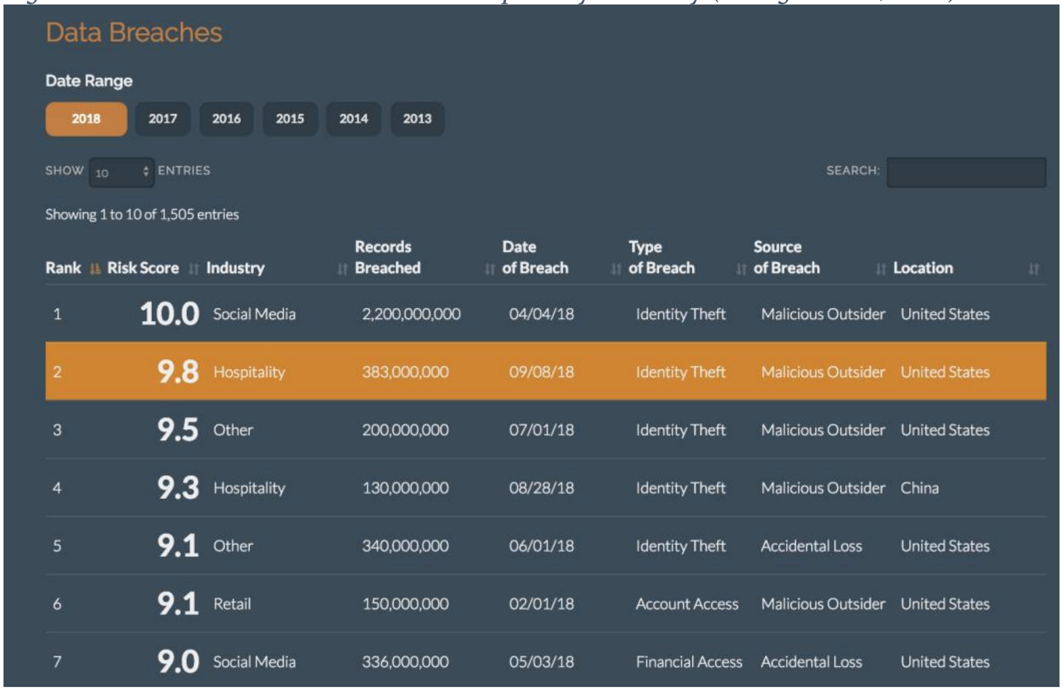


Figure 16 Data Breaches Within the Hospitality Industry (Bitsight.com, 2018)



Showing 1 to 10 of 1,505 entries

Rank	Risk Score	Industry	Records Breached	Date of Breach	Type of Breach	Source of Breach	Location
1	10.0	Social Media	2,200,000,000	04/04/18	Identity Theft	Malicious Outsider	United States
2	9.8	Hospitality	383,000,000	09/08/18	Identity Theft	Malicious Outsider	United States
3	9.5	Other	200,000,000	07/01/18	Identity Theft	Malicious Outsider	United States
4	9.3	Hospitality	130,000,000	08/28/18	Identity Theft	Malicious Outsider	China
5	9.1	Other	340,000,000	06/01/18	Identity Theft	Accidental Loss	United States
6	9.1	Retail	150,000,000	02/01/18	Account Access	Malicious Outsider	United States
7	9.0	Social Media	336,000,000	05/03/18	Financial Access	Accidental Loss	United States

Figure 17 Source https://breachlevelindex.com/data-breach-database

Standards/Legal

The market is saturated with guidelines, standards, regulations, frameworks, open or proprietary, with different purposes and different applicability, among which it is not always easy to orient oneself. Being able to choose the right points of reference and flexibly use them, personalising them according to the company's business requirements is as essential as it is often complicated for those not accustomed to this type of operation.

Different framework standards could be adopted when building a robust Information System. Below are some examples of IT security standards, laws and regulations, the application of which benefits from Cyber threat analysis:

STANDARDS

ISO/IEC 27001

It is now the most widespread standard for information security management within a public or private company. It requires the implementation of organisational and technical countermeasures that must be reviewed and improved cyclically considering the dynamic aspects that characterise the life of a company and the increasing threats that insist on its information systems. Clause 6.1.2 expressly requires the assessment of security risk.

The actual standard, which we call ISO 27001 was published in October 2005 and replaced the BS 7799 which changed its name to ISO 17799:2005 (the Code of Practice).

Its latest revision was published in 2013, and the full name of the standard is now ISO/IEC 27001:2013

(TechTarget, 2019)

The following ISO standard of 2007 is a collection of "best practices" that can be used to meet the requirements of the ISO 27001: 2005 standard and protect information resources.

ISO 27001 (the certification option) mandates the use of ISO 17799:2005 (the Code of Practice).
ISO 17799:2005 is the source of guidance for the selection and implementation of the controls mandated by ISO 27001

ISO 27001: objectives

The objective of ISO 27001 lies precisely in protecting data and information from all kinds of threats, ensuring their integrity, and availability to the sole and reserved "user".
The ISO 27001 standard dictates the requirements for the Information Security Management System (ISMS) which helps identify, analyse and address an organization's information risks to protect against cyber threats and data breaches, similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series). (Gerberding, 2017)
In the 2005 standard, however, the primary objective is to establish a system for the protection of IT information and management of risk.
It is based on a six-step planning process that involves collaboration between several different departments within an organisation:

1. Define a security policy.
2. Define the scope of the ISMS.
3. Conduct a risk assessment.
4. Manage identified risks.
5. Select control objectives and controls to be implemented.
6. Prepare a statement of applicability.

(Gerberding, 2017)

ISO 27001 is applicable public or private, profit or non-profit, regardless of their size or industry. However, it is necessary to consider that the adoption and management of an Information Security Management System requires a significant commitment of resources. For this reason, this system is often followed by a specific office (called, in jargon, "Organization and Quality office") composed of certified personnel. (ISO.org, 2019)

*Bespoke International Tour (Franchises) Ltd will develop its security posture based off of the ISO 17799:2005 Code of Practice (*ISO 14785:2014) *once it expands its business it will aim to obtain the Certification.*

Common Criteria - ISO/IEC 15408

The standard is widespread in numerous IT product/system certification schemes and offers the tools to specify, for a given operational context, the possible threats, the security functions that oppose them and the guarantees that these are correctly implemented. The standard requires defining the Security Issue by describing threats in terms of threat agents, actions of the agent's assets subject to such actions.

COBIT

It is a framework aimed at the governance of Information Technology to support corporate business processes. In its Cyber Security application, security risk analysis, the definition and categorisation of information sources and their collection are fundamental: attacks, breaches, accidents and statistics on them.

20 CIS (Centre for Internet Security)

Developed by the SANS™ Institute, "the CIS is a recommended set of actions for cyber defence that provide specific and actionable ways to stop today's most pervasive and dangerous attacks".
SANS can count on the help of professionals who are experts in information security, coming from the most prestigious universities, the leading companies and the most renowned research centres in the sector.
The main vulnerabilities of the network amount to more than one hundred, grouped into 20 categories, related to 7 different types of applications and programs susceptible to attacks. This subdivision is useful to provide security experts with guidelines to combat threats attributable to each group. (Gerberding, 2017)

BS31111

The standard aims to guide enterprise organisations regarding cyber risk and resilience, and to address the gap in IT decision making. (Microsoft, 2018)

CoSO (Committee of Sponsoring Organizations of the Treadway Commission)

The Internal Control System (ICS) is a fundamental element of the overall corporate governance system; it ensures that the business is in line with business strategies and objectives, is consistent with company policies, complies with the mandatory and voluntary requirements and is based on rules of sound and prudent management.
The report entitled "Internal Control: Integrated Framework", better known as the CoSO Report, came to life in 1992 and was updated in 2013. This framework, after confirming that the absence of a single definition of internal control had caused confusion and misunderstanding between the various subjects interested in the applicable procedures, outlined for the first time the fundamental characteristics, given the creation of a reference model for companies and other involved organisations. The internal control, based on the definition proposed by the CoSO, is a process (which involves the Board of Directors, managers and other operators of the company organisation) aimed at providing reasonable assurance about the pursuit of company objectives concerning the following aspects:

- compliance with laws, regulations and contracts;
- reliability and integrity of the financial statements and information;
- heritage protection;

- effectiveness and efficiency of operations

(CoSO.org, 2013)

NIST

The U.S. National Institute of Standards and Technology (NIST) represents the structure of the life cycle of the management process of cybersecurity, both from a technical and organisational point of view. The core is structured hierarchically in function, category and subcategory. The competing and continuous functions are:

IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER and constitute the main topics to be faced in order to operate adequate cyber risk management strategically. The Framework, therefore, defines, for each function, category and subcategory, the enabling activities, such as processes and technologies, to put in place to manage the single function. (NIST, 2019)

ISA 99 / IEC 62443

The United Nations Economic Commission for Europe, North America and Central Asia (UNECE, based in Geneva) have announced that it will use the ISA 99/IEC 62443 standard within the Common Regulatory Framework on Cybersecurity (CRF) which will represent its "official position" in terms of information security.

The IEC62443 is undoubtedly the most widespread standard at the international level for the protection against cyber risks of networks and control and remote-control systems in the industry as in utilities: the adoption of this standard by UNECE will further contribute to its diffusion and adoption where there are critical industrial systems. (Innovation Post, 2019)

LEGAL

GDPR

With the advent of the European Data Protection Regulation (GDPR) [1], repealing Directive 95/46/EC [2] in force until May 2018 and "harmonising" what was provided in the UK by the Computer Misuse Act (1990), GDPR becomes strategic and essential in terms of accountability. On top of the GDPR, there are other essential Acts to comply with, such as the BS31111, the Employment Act, Human Rights Act, the Data Protection Act (2018) [3] which replaces the 1998 Data Protection Act.

In general, the entire Regulation is based on two fundamental principles, which inspire the entire regulatory construct: the principle of privacy by design, and the privacy principle.

The principle of privacy by design aims to protect every personal data from the moment of determining the means or processes useful for processing, as well as that obviously at the time of the processing itself (through, for example, the "sub-principles" of pseudonymisation and minimisation of the data processed).

The privacy principle aims to ensure that, by default, only the personal data necessary for each specific purpose of the processing are processed and that it, therefore, affects the quantity of personal data collected, the scope of the processing, as well as the storage period and their accessibility.

Therefore, the Regulations require, above all, that personal data be processed in such a way as to guarantee adequate security, including their protection, through appropriate technical and organisational measures, from unauthorised or unlawful processing and loss, destruction or accidental damage.

Furthermore, the Data Controller must also be able to demonstrate that it has adopted this set of legal, organisational and technical measures aimed at protecting personal data in compliance with the provisions of the Regulation, including in terms of the effectiveness of security measures adopted. These measures, however, must take into account the scope of application, the context and the purposes of the processing, as well as the risk for the rights and freedoms of the natural persons to which the data belong.

Within the new legal framework outlined by the European legislator, there are no longer any minimum-security measures, but only adequate measures, designed by the Data Controller only after performing a risk analysis for each process performed.

Nevertheless, the Regulation in art.32 provides an illustrative list of the technical and organisational measures suitable to guarantee an adequate level of safety to the risk, which includes:

a) Pseudonymisation and encryption of personal data. (The Law Reviews UK, 2017)
b) The guarantee permanently of the confidentiality, integrity, availability and resilience of the processing systems and services.
c) The ability to promptly restore the availability and access of personal data in the event of a physical or technical accident.
d) A procedure to test, verify and regularly evaluate the effectiveness of the technical and organisational measures in order to guarantee the safety of the processing. (Firewallhardware.it, 2018)

DPIA

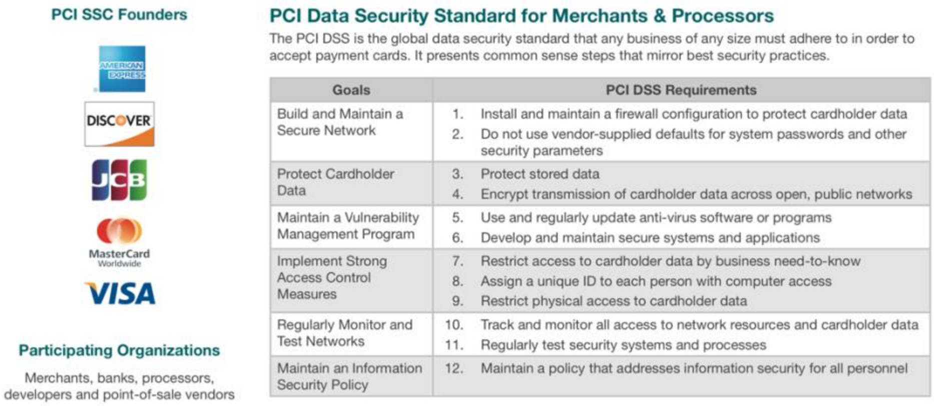
The art. 35, paragraph 7 of the GDPR defines and requires the Data Protection Impact Assessment (DPIA). The DPIA is a process aimed at the "assessment of the risks for the rights and freedoms of the interested parties". Therefore, the determination of threat profiles is particularly essential: actors, intents, motivations, techniques.

The DPIA should be seen as an essential and fundamental tool for all the owners and responsible for sensitive data in order to implement the new GDPR based on the principle of *accountability*.

PCI DSS

The GDPR Regulatory, the DAP 2018 are joined by industry standards and certifications such as the PCI-DSS. These three macro areas can be voluntary integrated with another security standard, ISO 27001, for an active, comprehensive and feasible information security program.

Compliance with the PCI DSS is a requirement for all operators who store, process or transmit credit card data. Developed by leading credit card companies, the Payment Card Industry Data Security Standard (PCI) DSS establishes measures to ensure consistent data protection and security processes for all online financial transactions.



PCI SSC Founders

AMERICAN EXPRESS
DISCOVER
JCB
MasterCard Worldwide
VISA

Participating Organizations

Merchants, banks, processors, developers and point-of-sale vendors

PCI Data Security Standard for Merchants & Processors

The PCI DSS is the global data security standard that any business of any size must adhere to in order to accept payment cards. It presents common sense steps that mirror best security practices.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Figure 18 PCI-DSS compliance controls & requirements

Companies that do not maintain PCI DSS compliance are subject to severe fines and penalties. (PCI DSS, 2019)

The PCI DSS compliance standard outlines 12 best-practice data security regulations for organisations that process and store payment card details, such as the use of SSL for network communications. (Gerberding, 2017)

The certification path is recommended to those who have a strong need to demonstrate compliance with these standards or to those who can effectively benefit from the business (e.g. the satisfaction of supplier requirements of some companies). This should be the main KPI, Key Performance Indicator, of the Information & Cyber Security: a number
expressed in pounds sterling that explains what investments have been made, or must be made, to protect the business by guaranteeing
more profits to repay the investments or avoiding unbearable losses. In terms of *accountability*, adopting this standard could be an excellent business strategy.

European NIS Directive

The NIS directive, with its recent national implementation, is intended "for both essential service operators and digital service providers to cover all related risks and incidents", and results in a joint effort by states members of the European Union, in order to guarantee a high and standard level of security of information systems and networks. It defines the need for adequate security measures and ever closer cooperation for the exchange of information, including characterisation of threats and incidents, and management practices of the same.

Computer Misuse Act (1990),

An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes. (Gov.UK, 2019)

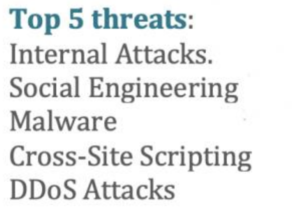
Data Protection Act (2018)

The UK's 2018 Data Protection Act is an almost identical copy of GDPR for a reason: when the UK leaves the EU, there will not be a massive shift in the law. After the UK leaves, GDPR will still protect the rights of EU citizens with businesses and organisations not having to change their policies.

However, there could be changes for organisations that move data between the European Economic Area and the UK. This depends on what deal the UK leaves with. Because the UK will not, technically, be part of GDPR, it does not have any assurances that data will be protected. As such, data adequacy becomes essential. At present, the UK government has said it will seek adequacy agreements with the EU to clarify that its data protection system is essentially the same as GDPR. Once agreed, this would mean that data could smoothly flow between the EEA and the UK. The ICO (Information Commissioner's Office) has produced guidance around this. (Burgess, 2019)

Generic top-level Security Framework

In order to tailor policies that will prioritise and tackle the five top threats Bespoke International Ltd will comply with the following Framework:



Top 5 threats:
Internal Attacks.
Social Engineering
Malware
Cross-Site Scripting
DDoS Attacks

Figure 19 Top Five threats

INFORMATION SECURITY POLICY

1.Overview

Incorrect use of IT tools involves serious risks, both for the employer and the workers. As far as the employer side is concerned, in order to safeguard the digitalised information assets and IT resources, it is necessary to prevent the creation, by the staff, of any abuses and damages in the use of the IT equipment supplied. As regards, instead, workers, given the enormous potential of these systems, it is a matter of preventing and avoiding potential remote controls, hidden and unjustifiably invasive, relating to the performance of the tasks assigned.
Therefore, the Company considers essential to define a clear corporate policy, governing the general rules for the correct use of IT equipment by staff, as well as collaborators who, in any case, have access to the Company IT equipment.

2. Purpose

The information must always be protected, whatever their form and in any case shared, communicated or stored. Information security and information protection from a wide range of threats, to guarantee business continuity, minimise risks and maximise investment and opportunity gains.

3. Scope

This policy supports the general organisation of information security policies.
This policy applies to the entire organisation.

4. Objectives

Strategic and operational risks to information security are understood and treated to reach an acceptable level for the organisation. The confidentiality of customer information, product development and marketing plans are protected. The integrity of accounting documents is preserved. Public web services and internal networks meet certain levels of availability.

5. Principles

The Company encourages risk analysis and therefore can tolerate risks that may not be tolerated in conservatively managed organisations, provided that risks concerning the information are understood, monitored and processed, if necessary, as required by the compliant Management System to the 27001 Standards.
All personnel are made aware of and responsible for the security of relevant information related to their role.
Resources have been allocated to finance information security controls.
In the overall management of the information system, the possibility of fraud associated with the abuse of information systems is analysed.
Objective evidence is available on the status of information security.
Information security risks are monitored, and appropriate actions are taken if any changes generate risks that are not acceptable to the organisation.
The criteria for risk classification and the level of acceptability are described in the Management System conforming to the 27001 standards.
Situations that put the Company in violation of laws and regulations will not be tolerated.

6. Responsibility

6.1 The Information Security Manager:

- Provides support for staff organisation
- Guarantees that the information on the security status of the information is available
- Acts in the event of an information incident

6.2 Each staff member has responsibility for information security as part of his or her job.

7. Key Results

7.1 The security incidents of the information will not entail serious and unexpected costs or interruption of services and commercial activities.

7.2 Losses due to fraud will be known and confined within acceptable limits.

7.3 Customer acceptance of products or services will not be adversely affected by concerns related to Information Security.

8. Related policies

For the correct implementation of the system, specific policies have been defined by the Company, gathered in the present framework.

ACCEPTABLE USE POLICY

1. Purpose

The purpose of this policy is to outline the acceptable use of the organisation's IT equipment. These rules are in place to protect personnel from the risks of improper use of the organisation's assets:

- Legislative non-compliance
- Virus attacks
- Compromise of network systems and services

2. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct business or interact with internal networks and business systems, whether owned or leased by, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at and its subsidiaries are responsible for exercising good judgment regarding the appropriate use of information, electronic devices, and network resources per the Company.
(Sans.org, 2014)

3. Policy

3.1 General Use and Ownership Policy

3.1.1 Users are responsible for promptly reporting theft, loss or unauthorised disclosure of confidential information.

3.1.2 Users can access, use or share proprietary information of the organisation only to the extent that it is authorised and necessary to perform their functions.

3.1.3 Employees are responsible for the personal use of the devices and, if the policy to be adopted is uncertain, must consult their supervisor or manager.

3.1.4 To guarantee the safety and the constant maintenance of the network, authorised persons within the company can monitor the equipment, the systems and the network traffic at any time.

3.1.5 The paper information must be kept in an adequately protected place/structure.

3.1.6 The organisation reserves the right to perform system and network audits periodically to ensure compliance with this policy.

3.2 Security and Proprietary Information

3.2.1 All mobile and computing devices that connect to the internal network must comply with the *Access Control Policy.*

3.2.2 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

3.2.3 All processing devices must be protected according to the "Clear Desk, Clear Screen" policy.

3.2.4 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware. (Sans.org, 2014)

3.3 Unacceptable use

3.3.1 The following activities are, in general, prohibited, except for specific exemptions, granted to carry out legal work responsibilities. In no event shall an employee be authorised to perform any illegal activity under local, state or international law, using resources owned by the organisation. Below is a list - not to be considered in any way exhaustive - of activities that fall into the category of unacceptable use in an attempt to provide a reference framework:

3.3.1 The violation of the rights of any person or company protected by copyright, trade secrets, patents or other intellectual property rights, or similar laws or regulations, including, but not limited to, "pirate installation or distribution "or without an appropriate license to use the software

3.3.2 The unauthorised copying of copyrighted material, including, but not limited to, digitisation and the distribution of photographs from magazines, books or other copyrighted material, copyrighted music, and installation of any copyrighted software, for which the organisation or end user does not have an active license is strictly prohibited. (Sans.org, 2014)

3.3.3 Access to the data of a server or account for any purpose other than business, even if we have authorised access, is prohibited.

3.3.4 The export of software, technical information, software or encryption technology, in violation of international or regional regulations, is illegal.

3.3.5 The introduction of malicious programs on the net or in the server (for example, viruses, Trojan horses, e-mails).

3.3.6 Reveal our account password to others or allow others to use our account. This includes the family when working at home.

3.3.7 Use an asset of the company to actively obtain or transmit material that violates laws concerning sexual harassment or the hostile work environment.

3.3.8 Make fraudulent offers of products, objects or services from any organisation account.

3.3.9 The implementation of security breaches or interruptions of network activity. Security breaches include, but are not imitated by:

- Access to the data of the employee is not a recipient.
- Access to a server or account to which the employee is not expressly authorised. For this policy, "business interruption" includes, but is not limited to:
- Denial of service: malfunction due to a cyber-attack that prevents the system from carrying out their ordinary activities

3.3.10 Port scanning or security scanning is expressly prohibited without prior notification.

3.3.11 The execution of any form of monitoring of the network that can intercept the data not intended for employee, unless it is part of the business activity.

3.3.12 Provide relevant information or lists of employees to external parties. (Sans.org, 2014)

4. Policy Compliance

4.1 Overview

The Company believes that the prevention activity should be prevalent over the control activity. It, therefore, undertakes to increasingly strengthen this prevention activity, in particular through awareness-raising and dissemination of the principles and rules to be observed in the use of IT equipment, in the adoption of specific technological solutions and any other measure deemed appropriate to that end.
The audits carried out by the Company comply with the following principles:

❖ Necessity: the data processed during the control activity are always and only those strictly necessary to pursue the purposes referred to in paragraph 1.

❖ Proportionality: the controls are always carried out in such a way as to guarantee, in individual concrete cases, the relevance and not excess of the information obtained concerning the purposes pursued and specified in paragraph 1.

❖ Impartiality: the audits are carried out on all the IT equipment made available by the company administration and consequently can involve all the collaborators as well, for whatever reason they use this instrument, except for that assigned to the Union representatives. In no case are targeted and repeated audits carried out against specific subjects with discriminatory or persecutory purposes.

❖ Transparency: based on this principle, the administration implements all the actions necessary to guarantee the prior knowledge of all the subjects potentially submitted to the controls of this regulation. All the subjects referred to in the previous point 2 are therefore informed of the possible checks.

❖ Protection of personal data: the checks are in any case carried out respecting the dignity and personal freedom of the subjects under control, as well as guaranteeing the confidentiality of the personal data collected during the control procedure. The data is known only to those previously designated as data controllers and processors. In addition to the above, the checks are carried out in compliance with the current legislation on the protection of personal data.

4.2 Purpose

The audits referred to in this framework are carried out for the following purposes:

- prevent improper or potentially harmful conduct for the Administration which may also involve the imposition of disciplinary sanctions.
- avoid or in any case reduce the risks of civil and criminal involvement of the Company, due to the contribution of a crime, in the case of offences against third parties committed through the improper use of the assets made available by the Administration itself.
- protect the image of the Company and those who work there.

4.3 Compliance Measurement

The Administration will carry out checks on the correct use of IT and electronic tools in compliance with the regulations in force, as well as in compliance with the UK Employment Act and, UK and Country's collaborator's laws.

The audits are carried out by the Security Officer with the help of technical assistance, even after reporting from the competent regional structures or judicial police bodies.

4.4 Exception

The Security team must approve any exception to the policy in advance.

4.5 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Related Policies

- Access Control Policy
- Data Classification Policy
- Data Protection Standard
- Social Media Policy

ACCESS CONTROL POLICY

1. Overview

The protection of access credentials is one of the fundamental principles of information security, in particular, the creation and management of passwords that constitute the main countermeasure to unauthorised access.

Given the provisions of the current Data Protection Act and, subsequently, taken up by the new European regulation in force from 24/05/2018, relating to the protection of individuals with regard to the processing of personal data - GDPR UE 2016/679, it is necessary to define adequate and appropriate protection measures for the processing and protection of users' personal data.

The purpose of this document is to define a procedure - the Company password policy - which establishes the criteria for the creation, use, storage and management of authentication credentials provided to users for access to the IT services provided.

In general, the IT services present in the Company identify, as an access tool for users, an authentication (and authorisation) system based on login credentials.

It consists of a code to identify the user ("username"), associated with a reserved keyword ("password") known only to the user. The two elements joined together, constitute the access credential ("account" or "user") as defined by current legislation on personal data.

2. Scope

The password policy applies to all central, management and application IT services, including web services, to workstations, to the wi-fi network, to the e-mail service and to all the applications and IT resources in the University that provide a system authentication for access, including the IT systems and resources present in the decentralized structures.

3. Policy

3.1 Responsibilities of System Administrators

3.1.1 System administrators must protect the confidentiality and integrity of passwords on the systems they manage and configure IT services, forcing the application where technically possible, to meet the requirements of this password policy.

3.1.2 The username is assigned, unless otherwise indicated, exclusively by the service administrator (or system administrator) or his delegate. The password is managed, after its first assignment by the administrator, exclusively by the user, except for cases where there are technical-organisational needs.

3.1.3 The identification code, once assigned to a user, can no longer be reassigned to other subjects, not even in subsequent times, precisely in order to guarantee storage and historicization of the utilities (as reported by the current legislation on the subject of personal data).

3.1.4 Access credentials that have not been used for at least 6 (six) months must be deactivated (unless they have been previously authorised as credentials for technical management purposes only, which therefore also require more extended periods of inactivity than the semester).

3.1.5 Credentials must be deactivated even when the user loses the role, the task and the qualities that allow him to use them to access the various services of the Company (e.g. termination of the employment relationship, transfer, demotion, dismissal, replacement).

3.1.6 Where there is a reasonable certainty that the user credentials have been used by someone other than the legitimate account owner, the same must be changed immediately by the user. In the event of inaction, this change will be made directly by the system administrator. The default passwords - such as those created for new users or assigned after a password reset - must be able to be changed by the user on first access. If technically possible, this password change must be imposed on the user by the system.

4. Password Policy

4.1 Users, once in possession of the credentials, must change the password at the first access according to the criteria described below, avoiding combinations that are easy to identify. Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own, personal accounts. (CPNI, 2015)

4.2 The password is strictly personal and must not be communicated or shared with any other person within the company, including local guides, assignees, collaborators, consultants.

4.3 Users must be careful not to provide their login credentials, not to respond to suspicious e-mails or to click on links while browsing the web (or in the mail) in order to not counter possible computer frauds (such as phishing, spear phishing, identity theft).

4.4 Each user is responsible for all actions and operations performed by his/her account.

4.5 If there is a reasonable certainty that the credentials assigned have been used by third parties, the user must immediately change the password.

4.6 For the safe storage of access credentials it is advisable to use a password management software (e.g. KeePass, LastPass, Dashlane), avoiding memorising them on sheets of paper, paper documents and files stored within the workstation. Such software also allows automating the login process to the various applications used.

4.7 If the user is blocked following the expiration of the password or if the password must be changed because forgotten or for any other reason, the user must use the self-service reset or password change services provided by the system or (if not available) contact the technical assistance service or the system administrator.

4.1. Technical requirements for creating and managing passwords

Definition - A Strong Password is defined as a password that is reasonably difficult to guess in a short time either through human guessing or the use of specialised software. (Carnegie Mellon University, 2017)

4.1.1 It must be no less than eight characters long or, if the system does not provide for it, a length equal to the maximum allowed;

4.1.2 Must be changed on first use and then at least every 6 (six) months;

4.1.3 Must contain, where possible, at least three characters between numbers, alphabetic characters in uppercase and lowercase, and special characters (e.g. B @ s13oLe);

4.1.4 Must always be different from at least the last four previously used;

4.1.5 Must not present a sequence of identical characters or groups of repeated characters;

4.1.6 Must be known exclusively to the user and cannot be assigned or communicated to others;

4.1.7 It must not contain references easily referable to the user or known areas;

4.1.8 Must not be based on names of people, dates of birth, animals, objects or words that can be derived from the dictionary (even foreign ones) or that refer to personal information;

4.1.9 Must not be stored in automatic log-in functions, in a function key or the browser used for internet browsing.

4.1.10 Automatic mechanisms of the system must impose the requirements of points 4.1.1 to 4.1.5.

4.1.11 For justified reasons of critical access to information, in case of an impediment of the credential holder, the password can be cancelled and replaced by system administrators with a new password.
In this case, the new password must be delivered by the system administrator to the user, who must change it at the first access.

5.Disabling the authentication profile

5.1 Failure to use the authentication credential for a period exceeding six months entails the automatic deactivation of the same. The user, to resume operations, will have to contact their Manager.

5.2 The authentication credential will be deactivated if the user terminates their relationship with the Company, as well as in the cases expressly and strictly required by law.

6.Disabling the authorisation profile

6.1 The authorisation profile granted to each user automatically expires every 12 months if it is not tacitly confirmed, or expressly cancelled before, by the respective Manager.

6.2 In case of change of duties or assignment, the verification is done by the Manager from time to time (Carnegie Mellon University, 2017)

5. Securing Workstations

5.1 Local computer privileges

There are three main categories of users on a computer or a network. These categories include:

5.2 *Limited User* → They can use computers and save documents but cannot change system settings.

5.3 *Standard User* → They can change system settings and install programs that do not involve operating system files.

5.4 *Administrators* → They have full access to read and write data on the system, add/remove programs or change system settings.

5.5 Most users on common networks must be classified as "limited user".

Only users with specialised training or needing further access should be allowed to change system settings and install programs that are not operating system programs. This is because many viruses, adware (software subsidised by advertising) or spyware (spy software) can be installed to deceive the user. If the user cannot install programs or change settings making them more vulnerable, most of these potential security problems can be avoided. (Best 7 Reviews, 2019)

5.6 The access level is closely linked to the user's role, can be changed only after demonstrating the absolute necessity for the performance of work functions, also must be approved by the information security manager before it can become effective.

5.7 Groups that can be admitted to a further type of access include:
Domain Administrators.
Software developers for testing purposes.

6. Network privileges

6.1 Most network users will be able to access the following types of network resources:

6.1.1 *Email* → Most users will have full access to their email. They will not be able to transfer the property to someone else.

6.1.2 *A personal storage space (drive) on a network file server* → This is a folder in a storage space that only the primary user of this unit can read and modify, except for domain administrators. The user will not be able to transfer the property to someone else.

6.1.3 *A drive shared by a group* → This is a drive and a folder that members of certain groups or divisions of the organisation can access. Access may be limited to reading or writing and may vary due to organisational needs.

6.1.4 *Access to databases* → There may be additional databases that can be stored on a shared drive or some other resource. Most databases have a standard usage level that allows users, with proper authorisation, to enter data and read report information. However, only database administrators will have full access to all the database resources they manage.

6.1.4.1 Groups that can be granted an additional level of access include:

- *Backup Operator*: he is allowed to read the data on the domain in order to save the files on the backup media. This group cannot modify the data of a domain.
- *Account Operator*: he can manage and view domain user account information.
- *Server Operator:* he has privileges concerning the servers, including reading and writing data, installing programs, and changing settings.
- *Domain Administrator:* he has privileges on all computers in the domain, including servers and workstations. Privileges include reading and writing data, installing programs, and changing settings. (blogs.technet.microsoft.com, 2016)

IT EQUIPMENT POLICY

1. Overview

All users undertake to use the IT equipment in compliance with the principles set out in this framework and to observe the following behavioural rules:

1.1 Use of the Internet/Wi-Fi

1.1.1 Access to the Intranet system resources from outside is allowed only through a connection that requires VPN (Virtual Private Network) authentication.

1.1.2 The connection to the Internet from company PCs must be made exclusively via the company network. Private modems cannot be used to connect to the network.

1.1.3 Access to the Internet provided by the Company is allowed only for work purposes and for access to data and information concerning the business; for personal reasons, access is allowed only in case of need and in any case not repeated or for prolonged periods, avoiding:

1.1.3.1 Accessing sites and/or acquiring and/or disseminating obscene information content, or damaging individual or collective good repute, or other potentially offensive or defamatory material. In particular, the receipt, transmission or possession of pornographic images is prohibited.

1.1.3.2 Participates in social networks (Facebook, Myspace, Twitter and the like), blogs, discussion forums if this is not directly linked to work activities falling within the scope of external company communication;

1.1.3.3 Stay connected to music sites for extended periods, even if at the same time user continue to work, as this can weigh down network traffic;

1.1.3.4 Download programs, even free ones, if this is not indispensable to the performance of the work activity, reporting it in advance to one's manager or computer assistance;

1.1.3.5 Access to services for recreational purposes or to chat lines;

1.1.3.6 Access to sites for sharing and streaming of multimedia content and the like, unless they are sites related to work. (Sans.org, 2014)

1.2 Use of the PC

1.2.1 In case the user leaves, even temporarily, the workstation, they must not leave the operating system of their PC open and must protect their computer by suspending or blocking the work session. At the end of the service time, before leaving the offices, collaborator must ensure that it has appropriately turned off the PC.

1.2.2 The users are responsible for the portable PC and any accessories assigned to them (camera, video projector) and must keep them with diligence, both inside the offices and outside until they are returned. Particular attention must be paid to the use and storage of the portable PC outside the network and offices of the Company (e.g. teleworking) in connection to external networks and in the removal of any personal files stored in the devices before returning them.
(Sans.org, 2014)

1.3 Use of email

1.3.1 Email is a work tool and, as such, should be used according to criteria of diligence and correctness, as well as based on the provisions of this Framework.

1.3.2 The assignment of email accounts implies the obligation to use this means of communication only for the performance of one's work activity.

1.3.3 The use of electronic mail of the Company is also allowed for private reasons and for inter-personal contacts (ex. to send or receive e-mails from a friend), but only if the following conditions are strictly stated:

- The emails must not be used for profit purposes (e.g. exchange of commercial data for another activity);
- The emails must not include contents that can create damage, even of the image, to the Company or illegal content and pornographic content;
- The use of electronic mail for purposes other than work is tolerated only outside working hours.

1.3.4 It is forbidden to install and use e-mail client systems that do not comply with the standards adopted by the Company.

1.3.5 The employee must not disclose his credentials for access to email and network services to anyone, nor use the username and password of other users.

1.3.1 The "everyone" formula as an e-mail recipient can only be used by executives or people specifically authorised by executives for a specific type of "everyone"*. It is expressly forbidden to use the "everyone" formula for sending prank emails, sending greetings of any kind (Christmas, etc.), computer chains and any other type of message not expressly provided for in this specification. We reiterate that the electronic mail tool cannot be compared to a forum to host discussions, comments, considerations of various kinds. The "everyone" formula can be used for trade union communications by internal trade union representatives, as well as for trade unions that, having the requisites foreseen to benefit from the trade union prerogatives foreseen by the reference legislation, have previously communicated to the institution the name of the employee authorized to forward communications through the company electronic mail.

1.4 Use of printers and consumables

1.4.1 The use of printers and consumables in general (paper, ink, toner, magnetic media, digital media) is reserved exclusively for work. Any waste of the materials mentioned above or excessive use must be avoided in any way.

* Example: a press release can be sent with everyone by the executive of the Press and External Relations Service or by personnel permanently delegated by him for this specific type of sending. Another example: an e-mail relating to an interruption of IT services for maintenance can be sent with everyone by the IT Service Manager or by staff permanently delegated by him for this specific type of sending.

SECURITY AND PRIVACY POLICY

1. When using computer equipment, the user should take the following precautions:

1.1 Keep the authentication credentials (passwords) secret, both those to access the equipment supplied and those to access the various programs used in the context of the work, assigned by the System Administrator;

1.2 It is forbidden to assign, once authenticated on the PC, the use of the workstation to unauthorised persons, in particular for access to the Internet and email services;

1.3 To adopt, in the course of work, the necessary precautions to ensure the security of the data processed and of the data that can provide useful information to a possible hacker;

1.4 All employees/collaborators must use, in case of processing sensitive data, the network folders or other storage media made available by the Company in order to guarantee the availability of the data also following errors or accidental events, thanks to the centralised backup system;

1.5 Provide appropriate measures that allow, in the event of absence from the workplace, other authorised users to access potentially necessary data (e.g. to save the data present on the hard disk in shared folders on file servers);

1.6 Do not connect external devices to the internal network of the Company (such as modems or routers) that could compromise the proper functioning of the corporate network;

1.7 Do not use instant messaging tools (e.g. Skype, Messenger) for personal reasons;

1.8 Do not introduce or distribute illegal programs (e.g. viruses, worms, spyware, ...) on the corporate network;

1.9 Do not take action in violation of the laws protecting intellectual property or copyright;

1.10 Use the mail made available to the Company for the working activity only, exclusively for the specific purposes of the same, in compliance with the functionality and security requirements of the information systems;

1.11 Do not use external e-mails in e-mail software (e.g. Outlook Express), as these involve risks for the security of the systems, while it is allowed to use external e-mails via the web for private purposes, provided in moderation and for short periods;

1.12 Take care not to open e-mail attachments from the sender or the suspected object to prevent the risks caused by malicious software (e.g., viruses, worms, spyware);

1.13 Limit to the minimum the dissemination of our company e-mail address on public websites (e.g. forums, mailing lists and the likes);

1.14 Do not remove the antivirus program installed on the workstation;

1.15 Check for any viruses before using removable media;

1.16 If the antivirus software detects the presence of a virus, suspend any processing in progress without shutting down the computer and signalling the event to the security and network and system management personnel; do not send e-mail messages containing virus reports to other users;

1.17 Use only the authorised software and supplied by the Company on the workstations; any additional software, compared to the standard installation, must be requested from the manager;

1.18 Do not leave corporate mobile devices unattended (such as mobile phones and tablets);

1.19 In the event of a security incident (such as in the case of unauthorised access or IT threats to the system), strictly follow the instructions received from the security and network and system management personnel;

1.20 When using certified electronic mail, the credentials (user id and password) to access this mailbox must be known only to the employees of the office authorised by the service manager.

1.21 Regarding the employees working at the Information System department, according to their job's tasks, point 1.1.4, 1.17 do not apply to them. (Sans.org, 2014)

COMMUNICATION POLICY

1. Purpose

This policy statement expresses the Company commitment to appropriate and effective communication to all stakeholders both internally and externally. It contributes a basic framework for planning and delivery and summary the roles and responsibilities of the different parties involved.

2. Scope

The Company is committed to the pursuit of knowledge and excellence and loyal to itself as a community of travel consultants. Communicating our mission and commercial goals should be underpinned by the principles of respect for difference and cultural diversity, transparency, equity and fairness with all stakeholders.

3. Policy

3.1 Management implement the following:

3.1.1 Informs the staff about the use of the resources of the information system of the Company, providing a copy of this regulation or specifying where it can be found on the website;

3.1.2 Ensure that everyone who works with the Company complies with the rules and procedures described in this regulation and report any infringements committed as well as concerning the consequent measures taken;

3.1.3 Assess the need to equip or not the personnel with IT tools, determine their profile for access to the information system and communicate subsequent changes to the System Administrator;

3.1.4 Collect and evaluate requests for access to systems and databases;

3.1.5 Periodically verify the employees on the use of the accesses.

3.2 The System Administrator is in charge of:

3.2.1 Monitor the systems to identify any incorrect use of the same in compliance with the privacy regulations and according to the provisions of this regulation;

3.2.2 Promptly notify the Manager of any unauthorised activity on the systems.

3.3 Each employee and collaborator in any capacity is personally and directly responsible for what concerns:

3.3.1 Compliance with the rules set out in this regulation;

4.3.2 Any use made of computer equipment and credentials assigned to it.

CLEAR DESK & CLEAR SCREEN POLICY

1. Purpose

To improve the security and confidentiality of information, the organisation has adopted a "clear desk" policy for clean documents and removable storage media, and a "clear screen" policy for the processing tools of the information. This is to reduce the risk of unauthorised access, loss and damage to information during and outside regular working hours or when areas are not operated. (NHS, 2010)

2. Scope

This policy applies to all personnel/collaborators/suppliers of the Company.

3. Clear Desk

3.1 Where possible, paper and computer media must be kept in safes, cabinets or other forms of protection when they are not in use, especially outside working hours.

3.2 The doors of the office areas must be locked when they are not in use or not supervised.

3.3 Confidential, sensitive or classified information, once printed, must be immediately removed from the printers. Where possible, printers with the password entry option for document protection should be used.

3.4 Use appropriate safety baskets to eliminate sheets with sensitive or personal information that is no longer needed.

3.5 Consider scanning documents and storing them on the PC.

3.6 Note that information left on the desk is more likely to be damaged or destroyed in an emergency such as fire, flood or explosion.

3.7 Do not print emails to read them: it only increases the amount of mess.

3.8 The reception desk can be particularly vulnerable to visitors. This area must be kept as "clean" as possible in every moment; in particular, medical records or other personal information should not be kept on the desk at visitors' reach.

3.9 Always clear the desk before going home.

4. Clear Screen

4.1 Users must ALWAYS "log-off" when they leave the computer unattended.

4.2 Set Windows Screen Lock to activate automatically when there is no activity for a short predetermined time.

4.3 The Windows Screen Lock must be password protected for reactivation.

4.4 Passwords should not be written down on/under the computer or in any other accessible location.

5. Monitoring and Revision Mode

5.1 All personnel are responsible for monitoring their compliance with the principles/procedures described in this policy. This policy will be subject to periodic review during the Management Review.
An exceptional revision can be justified if one of the following situations occurs:

- Company changes have occurred (e.g. statutory).
- Based on the results/effects of critical incidents.
- For any other relevant reason.

6 Non-compliance

6.1 All personnel must comply with this policy and, where required, to demonstrate such compliance. Failure to comply with this obligation will be considered as a disciplinary incident and will be treated accordingly.
(Sans.org, 2015)

BACKUP POLICY

1. Purpose

This policy defines the backup policies for computers within the organisation that need to back up data. These systems are generally the servers (file servers, mail servers and web servers) but are not necessarily limited to these.

This policy is intended to protect the organisation's data by ensuring that it is not lost and recovered in the event of equipment failure, intentional data destruction, or an emergency.

2. Scope

This policy applies to all equipment and proprietary data or managed by the Company.

3. Operating Modes

3.1 Definitions

3.1.1 *Backup* → The saving of files on an off-line storage medium (disconnected from the network), to prevent data loss in the event of equipment failure or destruction.

3.1.2 Archive → Saving old or unused off-line files in order to catalogue and lighten the system.

3.1.3 *Restore* → Process to report data stored off-line, in an online storage system such as a file server.

4. Times

4.1 Full backups are performed weekly. If for maintenance reasons, no Friday backups are performed, they must be made on Saturday or Sunday.

4.2 Archiving Backup media (if present)

It must be kept adequately in order to prevent damage.

5. Responsibility

Management must assign a member who is responsible for performing regular backups. The delegated person must develop a procedure to test the backups and test the data recovery capacity monthly.

6. Test

The ability to restore data from the backup must be performed at least once a month.

7. Backup Data

The data that needs to be backed up includes the following information:

- User data.
- System status data
- Registry

7.1 Backup systems include but are not limited to:

- File server
- Mail Server
- Web Production Server
- Database Production Server
- Domain Controller
- Database Test Server

- Web Test Server

8. Archives

8.1 Archives are made at the end of each year, in December. User account data, files and email servers are archived one month after leaving the organisation.

9. Restoration

9.1 Users who need their files restored must submit a request to the system administrator, including information about the file creation date, the name of the file, the last time it was changed, and the date and time when have been cancelled or destroyed.

RISK ASSESSMENT POLICY

1. Purpose

The objective of this policy is to ensure that the company reacts appropriately to any type, actual or presumed, of security risk relating to information systems and data.

The organisation is responsible for monitoring all risks that occur within it that may violate the security and confidentiality of the information. All accidents must be identified, reported, studied and monitored: the primary purpose of this policy is not to attribute blame, but to contain problems and learn from errors with a view to continuous improvement. (Doc Player, 2018)

1. Scope

This policy applies to all employees, contractors, consultants, temporary workers within the organisation.

3. Types of risks

The main risk categories are:

- **CRITICAL** risks must be reported immediately

e.g.

❖ Theft of documents
❖ Computer infected with viruses

- The **SIGNIFICANT** risks must be reported within 4 hours

e.g.

❖ Use of unlicensed software
❖ Unauthorised access and/or use of another user's access data

- **MINOR** risks must be reported within one day

e.g.

❖ Attempted penetration of defences
❖ Inappropriate email shipments

3.1 Types of risks

The Company recognises that there are risks associated with user access and information management systems in carrying out its activities; in fact, this policy aims to:
Reduce the impact of security breaches by ensuring that incidents are followed correctly.
Help identify areas for improvement to reduce the risk and impact of future threats.
Reduce the number of risks.

Non-compliance with this policy could have a significant impact on the efficiency of the organisation's operation and can cause financial losses, fines and the inability to provide the necessary services to our customers. (Sans.org, 2015)

4. Procedures to follow

4.1 Phase 1 →ACCIDENT DETECTION

An accident can and should be detected:
√ By operating personnel in carrying out their activities.
√ From the automatic alert of devices that monitor their system activities.
√ From the end user.

4.2 Phase 2 →RISK ASSESSMENT

4.2.1 The purpose of this phase is to determine quickly and precisely whether the risk is a serious one.

√ Data collection of the initial problem - the data is collected, and an appropriate impact classification is made.
√ Evaluation of the risk - the risk is assessed, and the Information Security Manager confirms the related category.
√ Serious accident - if the accident is classified as 'Critical', the assessment must be confirmed within 60 minutes of detection.

4.3 Phase 3 →RISK COMMUNICATION

4.3.1 The communication processes are intended to ensure that all parties are informed of the status of the risk.
Project managers and stakeholders must be informed of the risk and kept up to date on their progress to enable them to manage their customers.
In cases of serious risks, the Management must be informed and kept up to date.
If the violation could entail a high risk for the rights and freedoms of individuals, the Data Controller notifies the Guarantor within 72h from the moment in which it became known.

4.4 Phase 4 →RISK RESOLUTION

4.4.1 This phase includes all the various technical investigations that will be necessary to bring the incident to resolution; it may request the intervention of various technical and non-technical figures - resources are expected to be made available upon request.

4.5 Phase 5 →POST RISK RESOLUTION

4.5.1 The post-resolution process is started once the risk has been resolved.
Risk Review Critic: The Information Security Officer, on the occasion of a severe threat, calls a review meeting within three working days from the date of the resolution of the risk, in which the personnel involved participate.
Critical Risk Report: Develop appropriate options and action plans to reduce the threats of specific risks to project objectives. Conduct reviews to develop strategies for responding to risks. Update the Risk Register with the specification of the proposed response plan for the occurrence of each risk event and an updated Project Management Plan.
Non-Critical Risk:
It is reported by filling in a report signed by the Security Manager; no special meeting is required.
(Library Congress, 2015)

LOGICAL AND PHYSICAL SECURITY POLICY

1.Overview

This document has been prepared to take into consideration the best practices in the field of ICT (Information and Communication Technologies) management as well as the recommendations and applicable suggestions of the following main legislative, regulatory, Authority or trade association references:

1. Scope

This policy applies to all personnel/collaborators/suppliers of the Company.

2. Purpose

The reason of this policy is to define the main guidelines on logical and physical security in the management of information systems used for the management of sensitive data, such as customers addresses, email, phone numbers and credit card details. In particular, this logical and physical safety management procedure details the safety measures that the Company has taken concerning:

- Antivirus.
- Data backup and restore procedures.
- Management and control of physical access to the data centre.

3.1 Antivirus management and logical security

3.1.1 All PCs/servers present in the company and connected to the network, as well as entered in the Windows domain, are equipped with Antivirus with centralised management.
Antivirus uses a database of virus definitions known to identify malware and other threats on the PC. Employees of the data centre perform virus scanning updates, made available directly by the antivirus system, three times a week.
There are two firewalls set up to monitor network security:

1) ISA (Internet Security Accelerator) server from Microsoft, which acts as a proxy and/or client firewall.
2) Virtual Firewall, which also acts as a VPN and web termination filtering.

IT in the context of logical security will also carry out activities for the Company pseudonymisation using disjunction techniques. The personal/sensitive data is separated and made anonymous in order not to make an individual identifiable. This is used by the Company to allow suppliers to process their payments through a virtual credit card system. (Booking.com, 2018)

3.2 Behaviours to be adopted in the use of the antivirus

3.2.1 Each user must behave in such a way as to reduce the risk of attacks on the company computer system by either threat or by any other software not authorised by the Company.
In particular, it is forbidden for the user to download any software on the company PC.
Any software deemed necessary for the user's activity must be reported and authorised by the System Administrator.
If the antivirus software detects the presence of a virus that has failed to clean up, the user must immediately suspend the processing in progress, without turning off the PC, and report the incident to the System Administrator. (Inter Sistemi.it, 2010)

3.3 Management and Control of Physical Access to Data Centre

3.3.1 The company is equipped with 1 Data Centre:

3.3.1.1 Access is permitted only through the optical reader of the badge supplied to the Data Centre employees. The Data Centre is equipped with the following security measures:

- A video surveillance system to check for unauthorised intrusions.
- Armoured door, whose access control is monitored by an electronic badge.
- A paper control system, where each accessing user must sign the entry to the room.
- Gas fire protection system.

3.3.2 It is the precise duty of everyone, according to the functions and the relative responsibilities, that all the precautions to avoid undue intrusions in the company offices are scrupulously used, among which, in particular:

- Key locking of the Data Centre company room at the end of the working day and during the time of the employees' absence.
- Key locking of file cabinets and rooms inside the corporate Data Centre Office.
- Maintenance and control of the alarm system of the Administration building.

CRYPTOGRAPHY POLICY

1. Overview

All information, assets and resources of/or entrusted by the Company to third parties are protected against risks related to the respect of confidentiality, integrity and availability in proportion to their value and compliance with applicable laws.

The relevant data are protected from loss, destruction, falsification, unauthorised access and disclosure, in compliance with the legal, regulatory, contractual and business requirements, through specific technical tools and operating procedures described in the logical and physical security policy.

2. Scope

This policy applies to all personnel/collaborators/suppliers of the Company.

2. Purpose

The computer systems that use public communication channels (e.g., Internet network) are configured to perform encryption and decryption of the transmitted information. For communications between internal systems, the cryptographic keys can be generated by the systems dedicated to this operation by the Corporate Information Systems Area. The cryptographic keys used on systems that communicate with third parties are generated and managed by external Certification Authority. Both methods guarantee the same level of protection, guaranteeing the authenticity, confidentiality and integrity of the information transmitted.

The use of cryptographic tools is implemented in the context of full compliance with current legislation and accordance with regulations and agreements with third parties.

The systems used for the management of corporate information are located in secure premises, with controlled access. Protection is guaranteed by specific countermeasures to prevent the violation of confidentiality and integrity, both physical and logical, described respectively in the Logical and Physical Security Policy.

The Company adopts a policy of separation of IT environments dedicated to the development, testing and operation of its information systems, in order to reduce the risks of unauthorised access to information and changes or unavailability of operating systems.

The security of information that is managed outside the corporate information system is protected, through specific behavioural practices communicated through the Communication Policy.

MISCELLANEOUS

- Logical and physical security: a set of measures (of an organisational/technological nature) designed to guarantee the availability, integrity and confidentiality of information managed within the systems.
- Computer equipment: equipment for processing, managing and transmitting data and digital information: Personal Computer, server, storage, data transmission equipment.
- Antivirus: software designed to detect and eliminate computer viruses and other programs that damage the integrity of the network, data or attached devices.
- Firewall: indicates a hardware/software component which, using a specific set of predefined rules, allows filtering and possibly blocking all traffic to and from any computer network.
- Backup: data replication operation on any external support in order to prevent the permanent loss of data due to malicious or accidental unforeseen events.
- Restore operation to restore a system status, usually following a malfunction.
- User: authorised party (employee or external staff) to access an application
- NAS (Network Attached Storage): is dedicated file storage that enables multiple users and heterogeneous client devices to retrieve data from centralised disk capacity.
- Network: Set of hardware and software devices connected by specific communication channels, which allows the exchange of information and data from one user to another.
- Data Centre: a room where data servers are kept.

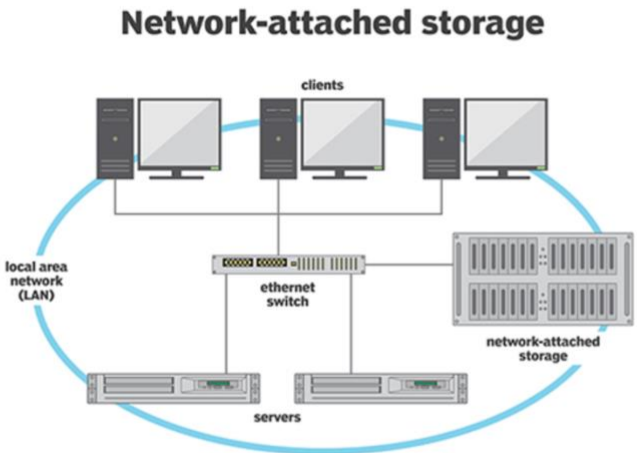


Figure 20 Network-Attached storage (Rouse, 2017)

- Software House/Suppliers: company specialised mainly in the production of software and applications.
- Domain: a network of computers that share a database of resources/data having common characteristics and united by a specific computer relationship.
- VPN: a private network that allows connecting securely and anonymously, using the internet, remotely concerning the work site.
- Proxy: In computer networks, a proxy creates a sort of defence barrier against the Web, acting as a filter for incoming and outgoing connections, as well as monitoring, controlling and modifying internal traffic.
- Honey Pot: In computer terminology, a honeypot is a system or hardware, or software component used as a "trap" or "bait" to detect, deflect, or, in some manner, counteract attempts at unauthorised use of information systems.
- IDS: The Intrusion Detection System monitor and analyse all the network activities, in order to find unusual data traffic and therefore, in this case, inform the interested user. In this way, the user can react to attempts of access by the intruder and block these attacks in the bud.
- IPS: The Intrusion Prevention System, as the name suggests, it goes beyond the Intrusion Detection System: after verifying the possibility of an attack, this type of system is not limited to informing the administrator, but immediately activates adequate security measures. In this way, they avoid having too long an interval between the detection of an intruder and the implementation of actions aimed at stopping it, as can happen with IDS programs.

(Cole & Northcutt, 2014)

Conclusion

The massive violations of financial institutions have led to a joint request for the regulation of personal information. These regulations are indeed an excellent approach, but they also represent a new problem for companies, as they must quickly adopt various international regulations in order to keep pace with consumer expectations about managing their personal information. Moreover, organisations, many of which have limited IT and security resources, will need to understand how to adapt to ensure compliance with these new regulations, while continuing to manage daily operations.

While on the one hand there is no doubt that the management of information security is different depending on the size of the company, it is possible to trace some basic principles that help to understand how to defend oneself effectively. A good security policy consists of at least five successive phases: identification (we need to understand which assets are to be protected and which threats), the provision of protection measures in an adequate manner (security checks and countermeasures, for example by installing firewalls and IDS), the detection of the malicious event (detection), the response - that is to unleash the defences to limit the damage produced by the attack - and, finally, the ability to recover, to restore the original conditions (for example thanks to the *Disaster Recovery Plan*).

More generally, one of the first things to put in place is to develop an internal culture: it is useless to install bombastic security measures if one's staff continues to click on anything received by email. Secondly, since the GDPR requires it and not only, a risk-oriented approach is needed.

A continuous risk assessment will be a fundamental aspect. As a result, compliance with these regulations is expected to play an increasingly important role in how organisations manage their risk profiles.

In case of implementing a new application or technology, companies will need to carefully consider their risk posture and, to address these challenges, they will need data management solutions that are automated, AI-based and result-oriented, if they hope to implement robust data privacy policies, without sacrificing productivity or agility.

With a sound system of effective prevention and regular scans, it is then possible to minimise the threat of data loss by cybercriminals. It is of paramount importance to then performs a regular backup, which allows continuity of access to information, which represents a critical key in IT security.

Online businesses must address IT security by starting from the basics: cybersecurity is increasingly a strategic priority for every company and organisation in the world, regardless of where the data resides. What has changed is the business model with which companies operate, which makes a leap in quality by security specialists inevitable, who must be able to guarantee the necessary support to their customers and create added value for their customers, mixing it with the right degree of innovation. Also because, in addition to hacker attacks, companies must beware of overcrowding in the world of security, which has about thousands of companies on the market. The security consultants, therefore, have the arduous task of selecting the most suitable for each specific business need, making the necessary integration of technologies and platforms as simple as possible.

A continuous risk assessment will be a fundamental aspect. As a result, compliance with these regulations is expected to play an increasingly important role in how organisations manage their risk profiles.

This is why companies should opt for technologies and software solutions that can efficiently address compliance with the GDPR.

The demand for managed security service providers at affordable prices will increase dramatically due to an increase in attacks on small and medium-sized businesses following the ransomware monetisation by criminal organisations. Small organisations finally realise that they have to be prepared like the big ones, in the field of computer security. Hackers take advantage of smaller organisations, which often feed the supply chains of large companies because they generally have security vulnerabilities that can be more easily exploited than more structured "targeted" companies.

Since security has not yet been well integrated into established industries such as utilities or healthcare, these sectors will be an easy target for attackers. The risk is that, although their vulnerability has been well documented, the industry does not take the threat seriously until a significant event occurs.

A risk assessment will, therefore, become an extremely critical topic for both the public and private sectors. Large organisations have already suffered huge losses due to decisions taken without effective corporate risk management. Data is a resource, but compliance with regulations regarding their protection is a cost to be taken into account and, in this sense, next year we will see the regulatory environment become even more complex around data governance, which will see the Enterprise Risk Management to establish itself as a priority for the top management of the companies. (Arc Media Global, 2018)

Bibliography

Acunetix, 2018. *Finger service running.* [Online]
Available at: https://www.acunetix.com/vulnerabilities/web/finger-service-running/
[Accessed 20 3 2019].

Arc Media Global, 2018. *Arc Medial Global.* [Online]
Available at: http://arcmediaglobal.com/60-cybersecurity-predictions-for-2019/
[Accessed 11 4 2019].

Best 7 Reviews, 2019. [Online]
Available at: https://www.bestsevenreviews.com/all-about-linux/
[Accessed 16 4 2019].

Bitsight.com, 2018. *Data Breaches Within the Retail and Hospitality Industries.* [Online]
Available at: https://www.bitsight.com/blog/data-breaches-within-retail-and-hospitality-industries
[Accessed 22 3 2019].

blogs.technet.microsoft.com, 2016. *Deploying Group Policy Security Update MS16-072 \ KB3163622.* [Online]
Available at: https://blogs.technet.microsoft.com/askds/2016/06/22/deploying-group-policy-security-update-ms16-072-kb3163622/
[Accessed 2 4 2019].

Booking.com, 2018. *Virtual Credit Cards,* Amsterdam: https://partnerhelp.booking.com/hc/en-us/articles/213317965-FAQs-Payments#link-6.

Boolean Logical Ltd , 2018. [Online]
Available at: https://www.boolean.co.uk/security-resources/
[Accessed 19 3 2018].

Burgess, M., 2019. *What is GDPR? The summary guide to GDPR compliance in the UK.* [Online]
Available at: https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018
[Accessed 25 3 2019].

Carnegie Mellon University, 2017. *Password Management.* [Online]
Available at: https://www.cmu.edu/iso/governance/guidelines/password-management.html
[Accessed 7 4 2019].

CERT Insider Threat Center, 2013. *Unintentional Insider Threats: The Non-Malicious Within.* [Online]
Available at: https://insights.sei.cmu.edu/insider-threat/2013/08/-unintentional-insider-threats-the-non-malicious-within.html
[Accessed 16 3 2019].

Chia, T., 2012. *Confidentiality, Integrity, Availability: The three components of the CIA Triad.* [Online]
Available at: https://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/
[Accessed 18 3 2019].

Cole, E. & Northcutt, S., 2014. *Honeypots: A Security Manager's Guide to Honeypots,* s.l.: Sans Technology Institute.

CoSO.org, 2013. *The 2013 COSO Framework & SOX Compliance.* [Online]
Available at: https://www.coso.org/documents/COSO%20McNallyTransition%20Article-Final%20COSO%20Version%20Proof_5-31-13.pdf
[Accessed 10 4 2019].

CPNI, 2015. *Password Guidance.* s.l.:Crown.

Dennis, J., 2018. *Travel staff are the weakest link in cybersecurity, says expert.* [Online]
Available at: http://www.travelweekly.co.uk/articles/314616/travel-staff-are-the-weakest-link-in-cybersecurity-says-expert
[Accessed 25 February 2018].

Digital Guardian, 2019. *Phishing Attack Prevention: How to Identify & Avoid Phishing Scams in 2019.* [Online]
Available at: https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams
[Accessed 21 3 2019].

Doc Player, 2018. *Security Incident Policy.* [Online]
Available at: http://docplayer.net/11029034-Security-incident-policy.html
[Accessed 10 4 2019].

Firewallhardware.it, 2018. *GDPR and pfSense / OPNsense. How to operate in order to be comply..* [Online]
Available at: https://www.firewallhardware.it/en/gdpr-pfsense-opnsense/
[Accessed 21 3 2019].

Frumento, E., 2018. *Social Engineering: an IT Security problem doomed to get worse.* [Online]
Available at: https://medium.com/our-insights/social-engineering-an-it-security-problem-doomed-to-get-worst-c9429ccf3330
[Accessed 21 3 2019].

Gerberding, K., 2017. *NIST, CIS/SANS 20, ISO 27001 – Simplifying Security Control Assessments.* [Online]
Available at: https://www.hitachi-systems-security.com/blog/nist-cissans-20-iso-27001-simplifying-security-control-assessments/
[Accessed 9 4 2019].

Gerberding, K., 2017. *Simplifying Security Control Assessments.* [Online]
Available at: https://www.hitachi-systems-security.com/blog/nist-cissans-20-iso-27001-simplifying-security-control-assessments/
[Accessed 10 4 2019].

Gov.UK, 2019. *Computer Misuse Act 1990.* [Online]
Available at: https://www.legislation.gov.uk/ukpga/1990/18/contents
[Accessed 11 4 2019].

Heidi Shey, S. B. B. B., 2016. *Understand The State Of Data Security And Privacy: 2016 To 2017.* [Online]
Available at:
https://www.forrester.com/report/Understand+The+State+Of+Data+Security+And+Privacy+2016+To+2017/-/E-RES136645
[Accessed 28 2 2019].

How to Stop DDoS, 2018. *7 nightmare cyber security threats to SMEs and how to secure against them.* [Online]
Available at: http://www.how-to-stop-ddos.com/7-nightmare-cyber-security-threats-to-smes-and-how-to-secure-against-them/
[Accessed 15 3 2019].

How to Stop DDoS, 2018. *Travel staff are the weakest link in cybersecurity, says expert.* [Online]
Available at: http://www.how-to-stop-ddos.com/travel-staff-are-the-weakest-link-in-cybersecurity-says-expert/
[Accessed 18 3 2019].

Huang, H.-C., Zhang, Z.-K., Cheng, H.-W. & Shieh, S. W., 2017. Web Application Security: Threats, Countermeasures, and Pitfalls. *IEEE,* 50(6), pp. 81 - 85.

INFOSEC, 2019. *Top 10 Anti-Phishing Best Practices.* [Online]
Available at: https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-countermeasures/anti-phishing-best-practices/#gref
[Accessed 21 3 2019].

Innovation Post, 2019. *ISA 99/IEC 62443.* [Online]
Available at: https://www.innovationpost.it/2019/01/22/cyber-security-lo-standard-isa-99-iec-62443-sara-adottato-su-scala-globale/
[Accessed 11 4 2019].

Inter Sistemi.it, 2010. *The code of ethics.* [Online]
Available at: http://www.intersistemi.it/the-code-of-ethics/?lang=en
[Accessed 8 4 2019].
ISO.org, 2019. *International Organization for Standardization.* [Online]
Available at: https://www.iso.org/standard/55038.html
[Accessed 9 4 2019].
Kaspersky Lab, 2019. *What is a Trojan Virus?.* [Online]
Available at: https://www.kaspersky.co.uk/resource-center/threats/trojans
[Accessed 2 3 2019].
Kerner, S. M., 2017. *Understanding Bring Your Own Device Security Risks.* [Online]
Available at: https://www.esecurityplanet.com/mobile-security/byod-bring-your-own-device.html
[Accessed 21 3 2019].
KLOSSNER, J., n.d. *JOHN KLOSSNER Blog Archive John Klossner: Everybody's doing it.* [Online]
Available at: https://fcw.com/Blogs/John-Klossner/2009/03/John-Klossner-Everybodys-Doing-It.aspx
Kraemer, S. C. P. &. C. J., 2009. *Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security, 28, 509-520..* s.l.:s.n.
Lewis, J., 2003. *Cyber terror: missing in action. Knowledge, Technology & Policy, 6, 34-41..* s.l.:s.n.
Library Congress, 2015. *RISK MANAGEMENT PLAN.* [Online]
Available at: https://www.loc.gov/portals/static/about/.../Risk_Management_Plan_Template.doc
[Accessed 9 4 2019].
Liginlal, D. S. I. &. K. L., 2009. *How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. Computers & Security, 28, 215-228..* s.l.:s.n.
McElhearn, K., 2016. *Viruses, Worms and Spyware—Yikes! A Look at Malware Terminology.* [Online]
Available at: https://www.intego.com/mac-security-blog/viruses-worms-and-spyware-yikes-a-look-at-malware-terminology/
[Accessed 20 3 2019].
MeriTalk, 2015. *Inside Job.* [Online]
Available at: https://www.meritalk.com/study/inside-job/
[Accessed 12 3 2019].
Microsoft, 2018. *Announcing: new British Standard for cyber risk and resilience.* [Online]
Available at: https://www.microsoft.com/security/blog/2018/04/04/announcing-new-british-standard-for-cyber-risk-and-resilience/
[Accessed 10 4 2019].
Microsoft, 2019. [Online]
Available at: https://www.microsoft.com/en-us/security
[Accessed 2 4 2019].
National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurit, n.d. [Online].
NHS, 2010. *Info Security Policy.* [Online]
Available at: https://www.fhft.nhs.uk/media/1520/info_security-policy.doc
[Accessed 2 4 2019].
NIST, 2019. [Online]
Available at: https://www.nist.gov/
[Accessed 6 4 2019].
NIST, 2019. *Framework Documents.* [Online]
Available at: https://www.nist.gov/cyberframework/framework
[Accessed 9 4 2019].
Ody, N., 2016. *Web filtering and monitoring – what do you need to know?.* [Online]
Available at: https://www.jisc.ac.uk/blog/web-filtering-and-monitoring-what-do-you-need-to-know-11-

jul-2016
[Accessed 18 3 2019].
Olavsrud, T., 2010. *9 Best Defenses Against Social Engineering Attacks.* [Online]
Available at: https://www.esecurityplanet.com/views/article.php/3908881/9-Best-Defenses-Against-Social-Engineering-Attacks.htm
[Accessed 21 3 2019].
OWASP, 2016. *Testing Guide Introduction.* [Online]
Available at: https://www.owasp.org/index.php/Testing_Guide_Introduction
[Accessed 19 3 2019].
OWASP, 2018. *Cross-site Scripting (XSS).* [Online]
Available at: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
PCI DSS, 2019. *Payment Card Industry Security Standards.* [Online]
Available at: https://www.pcisecuritystandards.org/pci_security/
[Accessed 6 4 2019].
Pfleeger, S. L. P. a. C. P., 2003. *Program Security*. [Online]
Available at: http://www.informit.com/articles/article.aspx?p=31782&seqNum=3
[Accessed 19 3 2019].
Platania, G., 2016. *DATA COMMUNICATION (Level 4) Assignment 1,* London : University of West London.
Ponemon Institute, 2017. *The Need for a New IT Security Architecture: Global Study on the Risk of Outdated Technologies.* [Online]
Available at: https://www.citrix.co.uk/it-security/resources/ponemon-security-study.html
[Accessed 28 02 2019].
Press, G., 2019. *60 Cybersecurity Predictions For 2019.* [Online]
Available at: https://www.forbes.com/sites/gilpress/2018/12/03/60-cybersecurity-predictions-for-2019/#ecb3bc543528
[Accessed 11 4 2019].
Proofpoint®, 2018. *The Human Factor 2018.* [Online]
Available at: https://www.key4biz.it/wp-content/uploads/2018/04/pfpt-us-wp-human-factor-report-2018-180425.pdf
[Accessed 2 4 2019].
Reason, J., 1990. *Human Error. Cambridge, UK:.* Cambridge, UK: Cambridge University Press..
Reason, J., 1997. *Managing the risks of organizational accidents..* Hants, UK: Ashgate Publishing.
Rogers, M., 2006. *A two-dimensional circumplex approach to the development of a hacker taxonomy. Digital Investigation, 3, 97-102..* s.l.:s.n.
Rouse, M., 2017. *Network-attached storage (NAS).* [Online]
Available at: https://searchstorage.techtarget.com/definition/network-attached-storage
[Accessed 10 4 2019].
Sans.org, 2014. *Consensus Policy Resource Community.* [Online]
Available at: https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy
[Accessed 3 4 2019].
Sans.org, 2014. *Consensus Policy Resource Community.* [Online]
Available at: https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy
[Accessed 3 4 2019].
Sans.org, 2015. *Security Risk Communication Tools.* [Online]
Available at: https://www.sans.org/reading-room/whitepapers/leadership/paper/36262
[Accessed 9 4 2019].
SecureLink, 2014. *Starwood breach shows the vulnerability of the hospitality and travel industry.* [Online]
Available at: https://www.securelink.com/blog/starwood-breach-shows-the-vulnerability-of-the-

hospitality-and-travel-industry/
[Accessed 14 3 2019].
SECUREWORKS, 2018. *Cybersecurity Awareness Training: Threats and Best Practices.* [Online]
Available at: https://www.secureworks.com/blog/cybersecurity-awareness-training-best-practices
[Accessed 16 3 2019].
Security Magazine, 2018. *89 Percent of Top Travel Websites Fail to Protect User Security.* [Online]
Available at: https://www.securitymagazine.com/articles/88974-percent-of-top-travel-websites-fail-to-protect-user-security
[Accessed 14 3 2019].
Shaqiri, A. B. -., 2014. *Management Information System and Decision-Making.* [Online]
Available at: http://www.mcser.org/journal/index.php/ajis/article/viewFile/2943/2903
[Accessed 18 3 2019].
Simmons, R., 2019. *BYOD Security Implementation for Small Organizations.* [Online]
Available at: https://www.sans.org/reading-room/whitepapers/mobile/byod-security-implementation-small-organizations-38230
[Accessed 10 4 2019].
Stallings, W., 2012. *Computer security : principles and practice..* Boston: Pearson.
Symantec , 2019. *What is a distributed denial of service attack (DDoS) and what can you do about them?.* [Online]
Available at: https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html
[Accessed 21 3 2019].
Symantec Corporation, 2019. *What Is A Computer Virus?.* [Online]
Available at: https://uk.norton.com/internetsecurity-malware-what-is-a-computer-virus.html
[Accessed 19 3 2019].
Symantec, 2018. *Threat Severity Assessment.* [Online]
Available at: https://www.symantec.com/content/en/us/about/media/securityintelligence/SSR-Severity-Assesment.pdf
[Accessed 10 4 2019].
TechTarget, 2019. *Understanding ISO 27001 and ISO 17799.* [Online]
Available at: https://searchitchannel.techtarget.com/answer/Understanding-ISO-27001-and-ISO-17799
[Accessed 9 4 2019].
The Law Reviews UK, 2017. *Privacy, Data Protection and Cybersecurity Law Review.* 4th ed. London: Alan Charles Raul.
Types List, 2015. *THE DIFFERENT TYPES OF COMPUTER VIRUSES.* [Online]
Available at: http://typeslist.com/different-types-of-computer-viruses/
[Accessed 19 3 2019].
TYPES LIST, 2019. *THE DIFFERENT TYPES OF COMPUTER VIRUSES.* [Online]
Available at: http://typeslist.com/different-types-of-computer-viruses/
[Accessed 16 3 2019].
Valbuena, J. K. a. I. L., 2016. *Excess XSS.* [Online]
Available at: https://excess-xss.com/
[Accessed 28 02 2019].
Veracode, 2019. *CRLF INJECTION TUTORIAL: LEARN ABOUT CRLF INJECTION VULNERABILITIES AND PREVENTION.* [Online]
Available at: https://www.veracode.com/security/crlf-injection
[Accessed 2 4 2019].
Walker-Roberts, S. & Hammoudeh, M., 2018. A Systematic Review of the Availability and Efficacy of Countermeasures to Internal Threats in Healthcare Critical Infrastructure. *IEEE Access* , 6(20 March 2018), pp. 25167 - 25177.

Wikipedia.org, 2019. *Cross-site scripting.* [Online]
Available at: https://en.wikipedia.org/wiki/Cross-site_scripting
[Accessed 16 3 2019].
Wood, C. &. B. J. W., 1993. *Human error: An overlooked but significant information security problem. Computers & Security, 12, 51-60.*. s.l.:s.n.
Zadelhoff, M. v., 2016. *The Biggest Cybersecurity Threats Are Inside Your Company.* [Online]
Available at: https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company
[Accessed 11 3 2019].
Nick Ismail (2017) https://www.information-age.com/7-nightmare-cyber-security-threats-smes-secure-123466495/
[Accessed:22/02/2019]
Buhalis, D., 1998, Strategic use of information technologies in the tourism industry, Tourism Management, Vol.19(5), pp.409-421.
Dieter Gollmann, 2011 – Computer Security, 3rd edition, Hamburg University of Technology
McAfee Labs Quarterly Threats Report www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf
Nick Ioannou. 2019 Internet Security Fundamentals, Boolean Logical Ltd
Sheldon, P. 1994. Information technology and computer systems. In Witt, S. and L. Moutinho, (eds), Tourism Marketing and Management Handbook, Second edition. London, Prentice Hall: 126-130.
Sheldon, P. 1997. Information Technologies for Tourism. Oxford, CAB.
Wayne, S. 1995. Tourism and technology: Approaching the 21st century, WTO News 2:7-10.
(CPNI December 2013) Social Engineering: Understanding the threat - https://www.cpni.gov.uk
[1] Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016,
[2] Directive 95 / 46 / EC, 2016, in https://gdpr-info.eu/art-94-gdpr/
[Accessed:13/3/2019]
[3] UK Data Protection Act (2018) http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
[Accessed:26/3/2019]