The Cyber Competences Act - a Vital EU Regulation Concerning Mandatory Certification of Critical Network and Information Systems' Operators across the European Union

Dănuț MAFTEI
National Cyber Security Directorate, Bucharest, Romania
dn.maftei@gmail.com

> ***MOTTO:***
> ***"Companies spend millions of dollars on firewalls and secure access devices, and it's money wasted because none of these measures use to address the weakest link in the security chain: the people who use, administer and operate computer systems."***
> **Kevin MITNICK**

Cybersecurity is vitally important to all critical network and information systems (Critical N&IS). Effective information security comprises multiple layers of defense working together to protect Critical N&IS. When developing a proper cybersecurity, the only considered are especially technical layers, but effective penetration attacks often involve a mix of both the social and technical vectors of attack. The fact that the human error is one of the vital layers that could be a potential weakness for any system that incorporates humans needs a special attention and should be handled at the EU level. Given the increasing number of incidents created by insufficiently trained operators, a strategic necessity arises: the mandatory training and certification of Critical N&IS' operators across the EU. This objective could be fulfilled through a new Regulation (The Cyber Competences Act) for laying down measures to complement achieving a high common level of cybersecurity within the European Union.

***Keywords**: Cyber competences, Human error, Vulnerabilities, Critical network and information systems, Certification*
DOI: 10.24818/issn14531305/28.2.2024.04

1 Introduction

As the digital era develops, cybersecurity has become a part of everyday life and it can affect anyone using and anything connected to the Internet or with capabilities to be accessed through any kind of medium, locally or remote. As man's activities become ever more inter-connected through the digital environment, cybersecurity related vulnerabilities increase and everyday life becomes more exposed than ever before.

The current cyber threat landscape is expanding, bringing about not only new opportunities, but also challenges, which require more coordinated, adapted and innovative responses in the European Union (EU) and EU member states (MS). More connectivity, a growing level of digital transformation, a greater number of digital services and devices, IoT market and software development increase cybersecurity risks, thus exposing our society to cyber threats and exacerbating the dangers faced by citizens, including vulnerable persons.

Cybersecurity is also vitally important to **network and information systems used by state institutions, critical information infrastructure, essential/important entities, citizens, private organizations and businesses alike** (hereinafter referred to as ***Critical N&IS***) and the number, sophistication, magnitude, frequency, and impact of cyber incidents are increasing and pose a major threat to their normal functioning.

Cyber incidents can impede the pursuit of economic activities in the internal digital market, generate financial loss, undermine user confidence and cause major damage to the economy and society. And the situation is more complex and dangerous when we talk about the cybersecurity of the supply chain.

Effective information security comprises several layers of defense which work together to protect information and access to Critical N&IS. The premise is that if one layer fails, the others could fail too. Technical layers such as firewalls, software patches, intrusion detection systems, anti-virus programs, and encryption are often the only areas that are taken into consideration in cybersecurity when developing a proper defense. However, **effective penetration attacks often involve a mix of both the social and technical vectors of attack**, with an accent on the first rather than the latter accounting for the majority of cyber-attacks performed. Indeed, the most significant vulnerabilities specific to information security are related to **human error – a vital piece of the layers existing for defending Critical N&IS** that could be a potential weakness for any system comprised of humans.

Humorous acronym has to be mentioned, it being chiefly used by tech savvy staff to underline that a problem is caused entirely by the fault of the user: ”PEBCAK” (”Problem Exists Between Computer And Keyboard”).

If an individual with malicious intent is able to bypass a system, he could avoid all of the other defensive layers designed to ensure information security [1]. The human factor is the one who gives a real value to the cybersecurity field. Unfortunately, when talking about cybersecurity, the human factor could also represent a vulnerability, a huge source of risk for organizations. Human error is still very much the reason behind the majority of cybersecurity problems, an untrained employee being able to compromise business security in multiple ways.

There’s no denying that man’s proclivity to committing mistakes makes him the weakest link in the digital world. No matter how strong technological defenses are, they can always be circumvented by determined attackers who eventually trick, influence or coerce someone with credentials into giving them access into sensitive network and information systems. That is the reason why serious human-related challenges to information security emphasize the importance of having strong and up-to-date cybersecurity practices in place. Also, it furthers the general necessity for people to periodically update and develop their related digital competences and skills necessary for filling the gaps which slowly but steadily erode between the baggage of knowledge they possess and the work-related cybersecurity needs and challenges that advance on a daily basis, faced by our societies and economies.

When discussing about human operators of Critical N&IS, in addition to cyber-based threats, there are additional challenges that must be overcome for ensuring physical security, as cybersecurity includes also essential human/physical elements. Policies set for maintaining a „clean-desk policy”, free from classified/confidential documents, for locking screens and IT systems when operators are away from the desk, for staff that does not use to display ID badges/credentials on offices and enforcing building access controls – these are all physical protection measures that should be incorporated by entities into the cybersecurity culture.

Because managing employee cyber risks is essential for organizations, state institutions, critical information infrastructure, essential/important entities and businesses, the type and quality of the training provided to operators of IT systems is of utmost importance.

Human factors related to aspects such as lack of training, of attention to detail, poor planning or ignorance are associated to the *accidental* or *unintentional insider* and are quickly becoming a growing concern to security professionals. Here, there is no malicious intent or prior planning, when comparing to “*insider threats*” who are dissatisfied with the organization they use to work for, or are motivated by financial gain.

Many human-operated cyber-attacks share common dependencies on security weaknesses, as attackers usually take advantage of an organization’s poor cyber hygiene. Although cyber criminals could be technically sophisticated and employ a wide variety of *Tactics, Techniques and Procedures* (TTPs), it almost always is possible to mitigate their malicious operations by implementing good cyber hygiene and by providing cybersecurity training for employees.

The insufficient training is the reason why there is a strong need for having a solid general approach to be followed by all sensitive organizations across the EU, which should do something more than cyber hygiene, i.e. to conduct mandatory training in order to obtain the proper certification of Critical N&IS' operators.

Proper training and certification of Critical N&IS' operators in EU will help mitigating the negative impact of the cyber malicious operations in peacetime as well as during times of war.

2 The recent main EU policies and legal framework concerning measures for a high level of security of network and information systems across the Union

A few pieces of EU policies and legal framework connected to the current topic have to be mentioned, they being complementary:

The ***EU Cybersecurity Act*** [2] aims to enhance the resilience and security of the national cyberspace and recognizes the importance of certifying ICT products, services, and processes. It establishes an **EU Cybersecurity Certification Framework** that enables the creation of tailored and risk-based EU certification schemes[1]. Meanwhile, it enhances the role of ENISA - the EU Cybersecurity Agency - that has to promote a high level of cybersecurity awareness in the EU, cyber-hygiene and cyber-literacy among citizens, organizations and businesses.

According to the *Cybersecurity Act [4]*, ”*in order to mitigate all the risks, necessary actions need to be taken to improve cybersecurity in the Union so that **network and information systems, communications networks, digital products, services and devices** used by citizens, organizations and businesses – ranging from small and medium-sized enterprises* […] *to operators of critical information infrastructure – are better protected from cyber threats”*.

As the EU Cybersecurity Act mentions [4] ”***Cybersecurity is not only an issue related to technology, but one where human behaviour is equally important****. Therefore, 'cyber-hygiene', namely, simple, routine measures that, where implemented and carried out regularly by citizens, organisations and businesses, minimise their exposure to risks from cyber threats, should be strongly promoted*”.

The ***Directive (EU) 2022/2555*** [6] on measures for a high common level of cybersecurity across the Union (***NIS 2 Directive***) provides the following definitions for a ”***network and information system***”:

”*(a)* ***an electronic communications network*** *as defined in Article 2, point (1), of the Directive (EU) 2018/1972* [7]*;*

(b) ***any device or group of interconnected or related electronic devices****, one or more of which, pursuant to a program,* ***carry out automatic processing of digital data;***

(c) ***digital data stored, processed, retrieved or transmitted*** *by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance*.”

Shortly, **network and information systems** are **IT&C infrastructures consisting of equipment, applications and digital communication networks**.

For several years, the European Union has been taking many steps towards providing a better cybersecurity for EU MS, its institutions, partners and citizens. For instance, the ***Directive (EU) 2016/1148 - Network and Information Security Directive (NIS 1)*** [8] is the first piece of EU-wide legislation on cybersecurity – aimed mainly to **achieve a high common level of cybersecurity across the EU**.

To respond to the increasing threats by cyber-attacks, the NIS 2 Directive replaced the NIS

[1] An EU cybersecurity certification scheme is a comprehensive set of technical requirements, rules, standards and procedures, agreed at EU MS level for evaluating the cybersecurity properties of a specific ICT product, service or process

1 Directive and thereby **strengthened the cybersecurity requirements**, addressing the security of supply chains, streamlining reporting obligations, and introducing more severe supervisory measures and stringent enforcement obligations, including harmonized sanctions across the EU. The expansion of the scope covered by NIS 2 Directive, **by obliging more entities and sectors to take measures**, is going to increase the level of cybersecurity in EU in the longer term.

According to NIS 2 Directive [9], "*Member States shall ensure that essential and important entities* ***take appropriate and proportionate technical, operational and organizational measures for managing the risks posed to the security of network and information systems*** *which those entities use for their operations or for the provision of their services*".

By reading the *Article 20/Governance* of the NIS 2 Directive, it could be noticed that the EU decision makers have already paid attention to a **better protection of essential and important entities by training their staff**: "*Member States shall ensure that the* ***members of the management bodies of essential and important entities are required to follow training****, and shall encourage essential and important entities to offer* ***similar training to their employees on a regular basis****, in order that they gain sufficient knowledge and skills to enable them to* ***identify risks and assess cybersecurity risk-management practices and their impact*** *on the services provided by the entity*" [9]. But these requirements are not defined very clear, seem to be not mandatory and there are not rules and procedures regarding coordinated measures across the EU or penalties imposed.

The ***Cyber Diplomacy Toolbox*** [11] is a joint EU diplomatic response to malicious cyber activities that contributes to conflict prevention, the mitigation of cybersecurity threats, and greater stability in international relations. It influences the behavior of aggressors.

With more and more devices connected to the internet, security and resilience are not sufficiently built in by design, leading to unsatisfactory cybersecurity. The ***Proposal for a Regulation on cybersecurity requirements for products and components with digital elements***, known as the ***Cyber Resilience Act*** [12], is also part of the regulative framework of the EU and has the objective to establish **minimum cybersecurity requirements for digital products, services, and processes sold in the EU**. It aims to ensure that digital products and services are more secure and resilient against cyber threats and incidents, reducing the risk of cyber-attacks.

As we observe, a great deal of effort is focused on ensuring better cybersecurity across the Union through regulation, certification, standardization, mandatory requirements, and procedures. However, there's still much to be done and, as it has been noticed during the current research, the EU still lacks the unequivocally regulated sector required to respond better as cybersecurity challenges increase and become more complex: **the one regarding specific competences needed by operators of the network and information systems in state institutions, critical information infrastructure and essential/important entities.**

Thus, additional efforts are needed and should be mandatory in order to further enhancing the EU capabilities enforced for responding to cyber threats of all scales and to complement the achieving of a high common level of cybersecurity across the Union, by introducing a new **Proposal of Regulation of the European Parliament and of the Council laying down measures on training and certification of Critical N&IS' operators**.

3 Cybersecurity and the human factor

3.1 Definitions

As is the case with all of man's activity, the *human factor*, as one of the cybersecurity layers, provides a real value to the cybersecurity field. Consequently, at the same time, the human factor represents the source of risks and vulnerabilities for most organizations.

Thus, we are faced with the conundrum of the human factor, which can be a ***weakest link*** or an ***unintentional/accidental insider threat*** [13] in the cybersecurity system, and meanwhile, it could be the ***first line of defense*** or, at the ***very least, an important asset*** for the organization.

In order to better mitigate the risks associated with human error and face cyber-challenges, a few aspects have to be taken into consideration:

According to Harlington [14], ”a ***weakest link*** is represented by a current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data and who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization’s information or information systems”. It is usually the individual with not enough training, not too computer savvy, who accepts low pay checks, sometimes works overtime or has habits that cause lack of attention. It could also be a simple PC operator, a secretary in the government, a governmental member, an IT system administrator, a general manager, an accountant, an employee of the critical information infrastructure, essential/important entities or of a company that is a part of the supply chain, contractors, or even consumers, cybersecurity experts, as well as other kind of IT operators.

3.2 Human-error related challenges faced by Critical N&IS and organizations

The human contribution to nowadays cyber incidents is very clear. Unfortunately, cybersecurity is not only an issue related to technology but it is also an area where **human behavior plays an important role**, in some cases even **more significant than technology**.

Actions/inactions specific to the weakest links are taking place due to human failure or limitations related to individual work performance and they are a result of a specific lack of knowledge and training of the person, combined with the absence of actual intent to cause harm. Besides factors such as time pressure exerted because of strict deadlines, level of task difficulty, cognitive elements (vigilance, mental workload, human information processing), actions or inactions without malicious intent have the potential to generate mistakes.

Through their actions/inactions, untrained employees could unintentionally expose to cyber threats (e.g. by downloading malicious software, clicking on infected links, inadequate patch management, bad implementation of information security policies [15], etc.) state institutions, critical information infrastructure, essential/important entities and organizations, supply chains, the digital market, the economy and homeland security in general. They could also be easily tricked or manipulated in the digital world by fake news or malicious intent actors.

The improper disposal of physical records, bad password/username hygiene, devolving log-in details as a result of social engineering or via introduction of spyware/malware, using out-of-date software, theft of intellectual property, information loss due to the misplacement of portable equipment (smartphones, laptops, USB drives, CDs, hard drives), deceiving phishing scams, using policies such as *Bring your own device* (***BYOD***) [16] for equipment that is not properly set, could also expose organizations to cyber-attacks.

Even more complications could arise in regards to other aspects related to human factors of misapprehension: misunderstanding the importance of the software, networks, systems and data within an organization, ignorance about the level of risk attached to the assets for which they are directly responsible, or a lack of understanding about how their actions could be putting the same assets at risk.

Errors in cybersecurity have terrible consequences, as we have seen in recent years with high-profile data breaches/exfiltration, misdelivery/the accidental disclosure of sensitive information to hackers, the disruption of Critical N&IS or other types of cyber incidents.

As shown by the World Economic Forum’s Global Cybersecurity Outlook 2024 - Insight Report [17], ”the cyber-skills and talent shortage continues to widen at an alarming rate. […] Half of the smallest organizations by revenue say they either do not have or are unsure as to whether they have the skills they need to meet their cyber objectives. […] 52% of public organizations state that a lack of resources and skills is their biggest challenge when designing for cyber resilience”.

Moreover, ”*the lack of necessary IT skills shown by those who use the organization’s electronic equipment leads to* ***vulnerabilities connected to cyber-espionage***” [18].

The random acts of the weakest link/unintentional insider are of greater potential concern for organizations as they typically have no motive, no direct intent and no prior indicators upon which to act. Unfortunately, the final result is still the same, and their actions/inactions can be as damaging as those perpetrated by the malicious attacker [19]. These mistakes can be very costly since they involve privileged insiders employed by organizations who often have access to the most sensitive information.

The success of cyber-attacks is achieved by exploiting vulnerabilities not properly addressed (they being specific to technology, procedure and human weaknesses). When the vulnerabilities become known, the authorities, producers or the cybersecurity companies issue warnings, updates and solutions. Despite that, due to user’s low level of cybersecurity education, culture and the lack of proper training of network and information systems’ operators, attackers could keep accomplishing their purposes.

In the context of emergent technologies and their rapid evolution, it is difficult to secure a proper level of training to ensure proficiency in cybersecurity of employees and managers and also to ensure cybersecurity for public authorities and private entities. The unceasing innovation in the field, characteristic of cybersecurity and cyberspace, generates a **constant need for staff training**. Furthermore, to better understand the cybersecurity risks, cyber challenges, their impact on activity, and also the measures that must be taken to avoid such cyber incidents, managers at all levels should also receive specific training [20].

3.2.1 Some statistics regarding the human error contribution to cyber security incidents

According to the IBM’s Cybersecurity Intelligence Index [21], during 2014, around 95% of all information security incidents involved the human error.

”Despite the majority of cyberattacks during 2016 were hacking and malware-related, three of the main five cyberattack were associated to human factors (human errors, social engineering through phishing emails or deliberate misuse). In 2015, 22% and during 2016, around 16% of all data breaches were related to phishing, spoofing or social engineering, while in 2017, human errors accounted up to 36% of all data breaches” [22].

During 2020, researchers from Stanford University and other top cybersecurity experts concluded that approximately 88% of all data breaches were caused by an employee mistake [23].

Egress’ Insider Data Breach Survey 2021 [24] revealed that 94% organizations experienced data breaches during 2020, with human error being the top cause of serious incidents, 74% organizations were breached because of **employees breaking security rules**, and 73% suffered serious breaches caused by **phishing**.

According to *2023 Verizon Data Breach Investigations Report*, 82% of data breaches involved a human element. More specifically, human error falls into two categories: **skill-based errors** and **phishing scams** [25].

The *2023 Data Breach Investigations Report* [26] underlines that 74% of breaches involved the human element, that including **social engineering attacks, errors, use of stolen credentials or privilege misuse**. It mentions that some of the **threats are accelerating and they can go from proof of concept to mass exploitation.**

The annual research carried out by a producers of encrypted-USB drives found that 70% of corporate breaches are a direct result of employee error or malicious intent. Meanwhile, a 2023 Gartner report on cybersecurity **predicted that, by 2025, a lack of talent or human failure will be responsible for over half of all significant cyber events** [27].

It is clear that, although cybersecurity should evolve and vulnerabilities diminish, we are more exposed than ever before.

3.3 Social Engineering and the human layer of cybersecurity

Social engineering is nothing new at all. It is a tool of psychological manipulation that has been used since the dawn of man. While cyberattacks are generally considered to be technical, successful cyber malicious operations employ social engineering TTPs to help identify, target and exploit vulnerabilities [28]. Indeed, the most significant vulnerabilities in information security relate to human error, effective penetration attacks being often social rather than technical and they use to account for a lot of cyber-attacks.

In order to face the threats arising as a result of the aforementioned human factor in the information security field, organizations should first start off from identifying and addressing its biggest threat, namely ***social engineering*** attacks such as pretexting, baiting, or tailgating.

Humans are usually the easiest targets for cybercriminals, as they can become the backbone of organizations without being properly trained in the cybersecurity field. Thus, people can be social engineered into clicking on malicious links or opening infected email attachments, could be tricked to disclose/offer sensitive information to attackers, to break standard security practices, scared into installing and running malware or even allowing unauthorized access to the organization's network. Once the Critical N&IS are infected, detecting and removing malicious software can be challenging.

In a few words, **social engineering is represented by the TTPs used by the cyber threat actors for exploiting human errors to achieve a malicious objective** [29].

Such TTPs could be ***technology-based*** (by involving a digital interface that attempts to achieve the desired outcome - pop-up windows, email attachments, etc.) and ***human-based*** (they involve a person-to person interaction to obtain the desired action). In both cases, social engineering uses human interaction for psychologically manipulating individuals through persuasion and deception in order to influence the target's actions [30]. Attacks that use social engineering use to differ from traditional hacking because they could be non-technical and do not necessarily involve the exploitation or compromise of software or systems [31].

Phishing activities are connected to cybercrime and they are currently one of the most common form of social engineering, with more than 3 billion spam emails sent every day. But some of the phishing campaigns aren't as effective and the success rate is not satisfactory without adding other forms of social engineering. For instance, according to statistics, the average click rate for a phishing campaign during 2021 was 17.8% [32], while phishing campaigns that were more targeted and added phone calls had an average click rate of 53.2% – 3 times more effective.

Nowadays, **cybercriminals use generative artificial intelligence tools to write their emails**, which well improve their phishing success rates. When a phisher is using a Large Language Model (LLM) [33], simple instructions are all it takes to make emails look as if they came from the intended sender, phishing emails being sophisticated, written carefully, without grammatical errors or other inadvertencies, tailored for the intended target. The amount of work needed to create an effective phishing message has been reduced greatly, and their number has gone up consequently. For instance, during 2022, there's been a huge increase in malicious phishing emails (**1,265% intensification in malicious phishing emails, and almost 1000% rise in credential phishing in particular**) [34]. Because of using AI, it is much harder for users to detect phishing emails, which could expose not only everyday users and their systems but even Critical N&IS infrastructure and operators. AI-based threats are rapidly growing and, according to statistics, **71% of email attacks created through AI go undetected** [35].

4 Case studies: unintentional insider threats around the world that exposed the organizations they belonged to

The following cases present serious challenges arisen because of human error and demonstrate the importance of having strong cybersecurity practices in place, as well as the need to constantly monitor and update them to ensure the protection of sensitive information. They also highlight the importance of good cyber training, education and awareness courses not only for Critical N&IS' operators, but for all organizations and citizens.

4.1 Case Study 1: Target Corporation

Target, a large retail corporation, suffered at the end of 2013 a massive data breach that exposed the personal data of about 40 million customers (including credit and debit card numbers). The breach was traced back to the company's point-of-sale system, which was initiated by a malware installed on the computers of its store operators. These operators were considered to be the "weakest link" in the Target's security system as their lack of training and awareness regarding cybersecurity practices allowed the attackers to penetrate the system.

The breach was estimated at around $252 million, including the costs for banks to reissue around 22 million cards [36].

4.2 Case Study 2: Home Depot

During September 2014, ***Home Depot*** (HD - also a major retail corporation) suffered a data breach that exposed information regarding over 55 million customers involved in payments. Similar to the Target breach, the attackers installed malware on the computers of HD's store operators, also the "weakest links" in the company's security system. That very large retail data breach had as a result hundreds of millions of dollars in expenses and lost business for HD.

4.3 Case Study 3: Equifax Agency

Equifax, a large credit reporting agency in the world, suffered during 2017 a massive data breach that exposed the personal information of around 150 million customers. The breach was traced back to a vulnerability in Equifax's web application software, which was exploited by attackers. Despite the fact that the vulnerability had been discovered and a patch was available for months before the breach occurred, nothing happened. Equifax's lack of action to address this vulnerability was due in part to the company's PC operators, considered even in that case the "weakest link" as they failed to properly maintain and update the company's security systems. The breach resulted in significant financial losses and harm to Equifax's reputation.

4.4 Case Study 4: Marriott International

At the end of 2018, because a vulnerability of the IT system, ***Marriott International***, a world's large hotel chain, suffered a massive data breach that exposed the personal information of around 500 million guests. Hackers accessed the Marriott's Starwood guest reservation database, which contained the personal information of the guests (names, addresses, emails, phone numbers, passport numbers, and credit card information). Investigators discovered that the attackers accessed the database by using login credentials of two employees who worked for the Starwood subsidiary. These credentials had not been changed or disabled after Marriott's acquisition of Starwood, allowing the attackers to penetrate Marriott's systems undetected.

This is yet another example of the dangers of weak security practices within organizations.

4.5 Case Study 5: Capital One

Other important data breach that compromised the security of an entire organization was the one suffered in 2019 by ***Capital One***, a US-based bank and financial services company.

A misconfigured firewall in Capital One's cloud computing environment allowed a former Amazon Web Services (AWS) employee to access unauthorized the Capital One's cloud-based data storage systems and steal the personal information of more than 100 million individuals (names, addresses, credit scores, social security numbers).

The incident was described as a "**classic example of human error**" and a failure of Capital One's internal controls and security processes.

4.6 Case Study 6: The SolarWinds Supply Chain Attack

The ***SolarWinds*** ("Solorigate") supply chain attack was represented by a massive cyber-espionage campaign that affected quite a big number of government agencies and private companies in the US and around the world. The attack was carried out by using a malicious software update for the SolarWinds Orion IT management tool, broadly used by organizations for network monitoring and IT infrastructure management, and was then distributed to thousands of SolarWinds customers and organizations worldwide. The backdoor allowed the attackers to gain access to the networks of organizations that had installed the update, leading to compromising many of them, to the theft of sensitive information (personal data, emails, login credentials, etc.) and the disruption of critical IT systems.

The SolarWinds hack took place in late 2020 and was discovered in early 2021 and it is a very good example of **how the weakest link in an organization can expose sensitive information and cause widespread damage** **[**37].

4.7 Case Study 7: FIN7 Mails Malicious USB Sticks to Drop Ransomware

Starting with August 2021, the FBI received reports regarding packages containing USB flash drives mailed using the US Postal Service and United Parcel Service to **US-based companies** (businesses in the transportation, insurance, and defense industry), hoping that devices would be plugged in, infect systems with malware and thus set them up for future ransomware attacks.

Actually, the malware was distributed by the cybercriminal group "**FIN7**" aka *Carbanak* or *Navigator Group*, the infamous, financially motivated cybercrime gang that was behind the ***Carbanak backdoor malware***. In the packages there were also included fake gift cards, letters, and gifts to entice targets to plug the USB flash drives into their electronic devices.

The FBI warned that attackers were impersonating Health & Human Services and/or Amazon to mail poisoned USB devices to the targeted companies for executing a BadUSB attack.

That represents a highly effective cyber-attack using the art of social engineering, given the packages' "personal" touch to increase perceived legitimacy, as well as the general user's ignorance when it comes to **cyber threats delivered by physical means**. Malware distribution via physical devices is rare, because it requires additional operational and logistical resources, but that is not valid for **highly sophisticated threat actors** [38].

In all the cases, the weakest link was represented by operators who failed to properly secure and manage the network and information systems, leading to the exposure of sensitive information, personal data and the compromise of Critical N&IS. These incidents highlight the importance of having robust IT security measures, regular security assessments, clear protocols, information security policies and procedures to be followed, as well as employees training in preventing data breaches and cybersecurity.

5 The current initiatives on cybersecurity competences certification

In the EU, there are some initiatives on cybersecurity competences certification, as follows:

5.1 European Cybersecurity Skills Framework

Having the mission of promoting a high level of cybersecurity awareness in the European Union, including cyber-hygiene and cyber-literacy among citizens, organizations and businesses, ENISA has worked on developing the ***European Cybersecurity Skills Framework*** (ECSF) [39], which is intended to strengthen the EU cybersecurity culture by providing a common language across communities, taking an essential step forward towards Europe's digital future and development.

The ECSF has the objective to provide a practical tool to support the identification and articulation of tasks, digital competences/skills, and knowledge associated with the roles of European cybersecurity professionals. Its main purpose is to create a common understanding between individuals, employers and providers of learning programs across EU MS, making it a **valuable tool to bridge the gap between the learning environments and cybersecurity professional workplace**.

5.2 ICDL Europe

ICDL Europe [40] is an international organization dedicated to raising digital competence standards in the workforce, education and society. The certification programs, delivered through an active network in more than one hundred countries, enable individuals and organizations to assess, build and certify their competence in the use of computers and digital tools to the globally-recognized ICDL standard.

The ***European Computer Driving License*** (ECDL) is a certification available for all ages proving that an operator has basic knowledge/skills to use a computer, valid in all EU MS. The ECDL system, adopted as an international standard for some governments, is **mandatory for testing operators in state institutions and private companies within some EU MS**.

5.3 The Cyber Citizen Initiative

An EU financed project for the period 2022–2024 is the ***Cyber Citizen Initiative*** [5]. It intends to produce a model for cybersecurity learning and a learning portal based on that model in EU-wide collaboration, to improve citizens' abilities to act in a safe and secure manner in the digital world by using educational and communicative elements in the learning portal and to support EU's digital skills and capabilities development activities.

5.4 The Cyber Security Competence and Certification Centre – Slovakia

The Cyber Security Competence and Certification Centre (KCCKB) [10] unites the Slovak community and creates standards for assessment, education and European projects in cyber security. Addressing the education pillar, the KCCKB is involved in educational programs for cybersecurity managers and auditors and raising cyber security awareness among the general public.

Despite these quite effective and dedicated initiatives, it is easy to notice that the cybersecurity segment analyzed during the current research effort still remains partially covered. As mentioned before, additional efforts are needed for further enhancing the EU capabilities to respond to cyber threats of all scales and to complement the achieving of a high common level of cybersecurity knowledge and good practices across the Union by **introducing a new Regulation for training and certification of Critical N&IS' operators**.

6 A real need for the EU Cyber Competences Act

When it comes to cybersecurity, successful organizations should pay attention to people, processes and technology. Even though technology offers automated safeguards and processes to determine and control the needed actions to be taken in order to achieve a specific end, organizations (including entities with strong security practices) could face vulnerabilities caused by the human error, it still being very much the driving force behind the majority of cybersecurity problems [3]. Human error plays a key part in cybersecurity breaches/data exfiltration, loss of sensitive information, disruption of critical network and information systems, or in exposing the supply chain or other important organizations to cyber threats.

Given the high stakes involved in the cyber space, it is imperative that Critical N&IS' operators receive proper training to ensure they are armed with the necessary knowledge and digital skills to effectively defend countries against cyber threats.

Governments and other important organizations can sometimes neglect the idea that important employees may be the weakest link when operating Critical N&IS, eventually exposing their organizations to cyber threats. Management at all levels must be aware that a huge number of cybersecurity breaches and risks are generated by human mistakes and that they can be reduced through education, training and specific regulations.

Expecting that operators of Critical N&IS are going to train by themselves or that organizations pay enough attention to the training of their employees in order to better detect and respond to cyberthreats certainly isn't the best approach to cope with an ever-evolving threat landscape.

That is the reason why EU institutions should take on the responsibility of providing a regulation framework for laying down measures that aim to periodically conduct training and certification of employees, in order to ensure they are adequately prepared to identify and protect Critical N&IS against cyberattacks.

So, despite the complex EU policies and legal framework, additional efforts are needed for further standardization and enhancing the Union's capabilities to respond to cyber threats of all scales, and that could be done **by introducing mandatory regulations for EU MS concerning a *Cybersecurity Competences Certification Framework* for Critical N&IS' operators**.

The professional training programs developed on the basis of the aforementioned framework would be aimed particularly at those who perform activities in the cybersecurity field at the level of Critical N&IS, in order to ensure a consolidated technical expertise level related to threat evolution and in accordance with the current technological development, and also to inspire a well-organized professional behavior in preventing, countering and reacting to cyber-attacks and to cybersecurity incidents.

In a nutshell, training and certification of Critical N&IS' operators is vital for fighting against cyber threats. With the increasing reliance on technology, it is very important to ensure that the human factor gradually ceases to be the weakest link in the security chain. Effectiveness, adaptability, and flexibility should be pursued, and the development of an **EU Cyber Competences Act** is important to manage the risks implied by exposing the human factor to the cybersecurity field, while enabling the adoption and use of new technologies by EU MS.

A future EU Regulation regarding the training and certification of such operators should:

- lay down the main horizontal requirements for the **EU Cybersecurity Competences Certification Framework**;
- provide a comprehensive set of mandatory measures, rules, technical requirements, standards and procedures at EU level in order to improve the specific cyber competences and skills of such operators, and also to enable their certification;
- support the designated authorities in preventing, countering, investigating and diminishing the risks specific to cyber-attacks on Critical N&IS.

These efforts must be focused on staff specialization for:

- understanding the potential threats existing in cyberspace;
- maintaining a working knowledge regarding the rapid trend of technological developments;
- acquiring the necessary knowledge for an adequate reaction in case of cyber-attacks or cybersecurity incidents;
- developing necessary competences for responding to cyber incidents faced within the Critical N&IS operated on;
- being adaptable and constantly linked to the level of cyber threats.

Knowing that the partner organizations in EU and EU MS have a responsible behavior and train properly their employees could have a positive impact on building trust, improving cooperation and sharing information on cyber issues. Certification can serve also as a powerful tool for state institutions and important organizations to demonstrate their commitment to cybersecurity. It shows that they have taken the necessary steps to protect their systems and data, critical systems, partners of the supply chain, their customers' information, as well as the citizens and services provided to them. This can also provide a competitive advantage in today's marketplace. Furthermore, a proper training and certification of Critical N&IS' operators will develop a culture of security within an organization. By making training and security awareness a priority, organizations can foster a sense of responsibility among their employees and encourage them to take an active role in protecting their critical systems and data.

7 Conclusions on the need for an EU Regulation concerning mandatory training and certification of critical network and information systems operators across the Union

Cyber-attacks often target Critical N&IS around the world, including those relevant to national security. Maintaining continuity, integrity and availability in good order and ensuring their resilience helps insure optimal conditions of all areas of the economic and social life.

One of the key challenges faced by our societies and digital markets all over the world is related to the insufficient offer of relevant cyber competences needed to prevent, deter, detect and react to cyber incidents. There is a lack of skilled and qualified personnel to take on roles in cybersecurity and who can address in a safe and secure way the continuously evolving cyber threats and the emerging cybersecurity challenges.

The shortage of cybersecurity competences has several fundamental drivers, including an unsatisfactory level of understanding of the competences required in the cybersecurity discipline between different actors, and it needs to be addressed for a more cyber secure EU.

The level and the quality of competences specific to cybersecurity are relevant to maintaining secure and resilient Critical N&IS against cyber-attacks at the EU level. In this respect, it is necessary to develop certification, compliance and standardization mechanisms in the field of cybersecurity, which must consider a strict set of criteria - technical and non-technical.

Trained employees are **the first line of defense** when it comes to preventing cyber-attacks against Critical N&IS. Well-trained employees can quickly identify a threat when they see one and deflate any potential attacks from escalating into a disaster. Moreover, proper training of the human factor could replace the lack of quality IT personnel that would have to be well paid.

Statistics show that, **in the cybersecurity field, vulnerabilities increase proportionally to the evolution of technology, making our societies more exposed than ever before**.

The challenges that poorly prepared operators pose to Critical N&IS need special attention that should be dealt with at the EU level, as member states should realize that even a seemingly minor mistake can snowball into a terrible security disaster for strategic organizations, under the right circumstances and wrong incident reports. The situation exacerbates because more and more critical IT systems are becoming vulnerable to cyber-attacks as they get connected to electronic networks and that is exactly why the human factor is of strategic importance in cybersecurity and becoming a vital layer for protecting Critical N&IS.

Given the continuously increasing number of incidents created by insufficiently trained operators, a strategic necessity arises: the **mandatory training and certification of critical network and information systems operators across the European Union**.

It's time for EU and EU MS **to seriously consider the above-mentioned challenges related to human error in the cybersecurity field and to act by adopting proper measures**, managing risks related to operators in information security being essential and as well a way to create the best defense for organizations.

Although a great deal of research has been devoted to the exploration, categorization of, and countering threats posed by malicious attacks on Critical N&IS that are related to human factors and exploit human mistakes, just a few have presented a concrete proposal regarding the mandatory training and certification on cybersecurity competences at the EU level.

This objective could be fulfilled through a **Regulation** that lays down measures to complement achieving a high common level of cybersecurity across the EU, with a view towards improving the functioning of the internal market, i.e. a **Regulation of the European Parliament and of the Council laying down measures on training and certification of network and information systems operators in state institutions, critical information infrastructure and essential/important entities - *the Cyber Competences Act*.**

Because the EU needs highly qualified N&IS' operators, sufficiently trained and skilled, the **Cyber Competences Act** should provide the necessary tools for a high common level of cybersecurity across the Union and to be applied to Critical N&IS.

Developing cyber competences is an essential investment for the European Union and EU MS. The return on investment will be seen in the form of employees making better work-related decision, efficiently responding when facing of challenges and malicious actors, a better protected EU as a whole, saving businesses from data breaches, financial losses, damage to reputation and potentially expensive lawsuits.

Proper training and certification of Critical N&IS' operators is aimed at considerably reducing the impact of malicious cyber-attack operations, both during peacetime and times of conflict, being an essential investment for the European Union and the people of the member states.

References

[1] European Security and Defence College, Rehrl, J. (2018). *Handbook on cyber security*. Volume V, Rehrl, J. (editor), Publications Office, p. 190 [Online]. Available: https://data.europa.eu/doi/10.2855/3180.

[2] European Parliament, Council of the European Union. (2019, Apr., 17). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0881.

[3] F. Howarth. (2014, Sep. 2). *The Role of Human Error in Successful Security Attacks*. Securityintelligence.

[4] European Parliament, Council of the European Union. (2019, Apr., 17). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[5] Cyber Citizen. *EU-Wide Cyber Citizen Skills Initiative* [Online]. Available: https://cyber-citizen.eu/en/.

[6] European Parliament, Council of the European Union. (2022, Dec., 14). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and re-pealing Directive (EU) 2016/1148 (NIS 2 Directive) [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[7] European Parliament, Council of the European Union. (2018, Dec., 11).

Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [Online]. Available: https://eur-lex.europa.eu/eli/dir/2018/1972/oj.

[8] European Parliament, Council of the European Union. (2016, Jul., 6). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L1148.

[9] European Parliament, Council of the European Union. (2022, Dec., 14). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and re-pealing Directive (EU) 2016/1148 (NIS 2 Directive),).

[10] Cyber Security Competence and Certification Centre [Online]. Available: https://cybercompetence.sk/en/?_gl=1*1uiirdz*_up*MQ..*_ga*ODU2ODQ5MjY3LjE3MTM1MzEzNzY.*_ga_KJWSQW4FXH*MTcxMzUzMTM3NC4xLjAuMTcxMzUzMTM3NC4wLjAuMA

[11] Council of the European Union. (2023, June, 23). ”Revised Implementing Guidelines of the Cyber Diplomacy Toolbox” [Online]. Available: https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf.

[12] European Commission (Proposal). Proposal for a Regulation on cybersecurity requirements for products and components with digital elements [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

[13] The threat posed by a current employee who, without malicious intent, causes a breach in organizational cybersecurity.

[14] L. Hadlington, ”The “Human Factor” in Cybersecurity: Exploring the Accidental Insider", in Psychological and Behavioral Examinations in Cyber Security”, *International Journal of Computer Science and Information Security (IJCSIS)*, De Montfort University, UK: IGI Global, 2018, p. 51 [Online]. Available: DOI: 10.4018/978-1-5225-4053-3.ch00; https://www.academia.edu/66124882/The_human_factor_in_cyber_security.

[15] Some of the information security policies are: Acceptable use; Network security; Data management; Access control; Pass-word management; Remote access; Vendor management; Removable media, etc.

[16] Using for official purposes personal devices without the same level of security protection as the organization's devices.

[17] World Economic Forum. (2024, January). *Global Cybersecurity Outlook 2024 Insight Report*, p. 4 [Online]. Available: https://www.weforum.org/publications/global-cybersecurity-outlook-2024/. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.

[18] D. Maftei. (2015, Apr.). ”Risks, Threats and Vulnerabilities Related to EU Classified Information within CSPD Missions and Operations”, *SSRN, National Strategies Observer, Institute for World Economy, Romanian Academy* [Online]. No.1/Vol.1, vol. 1, p. 165. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2637122.

[19] L. Hadlington, ”The “Human Factor” in Cybersecurity: Exploring the Accidental Insider", in Psychological and Behavioral Examinations in Cyber Security”, *International Journal of Computer Science and Information Security (IJCSIS)*, De Montfort University, UK: IGI Global, 2018, p. 51.

[20] Romanian Government. (2021, Dec. 30). *HG 1321/2021 for approving the Romania’s Cyber Security Strategy 2.0 for*

2022-2027, as well as of the Action Plan for the Implementation of Romania's Cyber Security Strategy for 2022-2027, Chapter 1 – Introduction, Section 1.4 – Enabler factors of cyber threats [Online]. Available: https://legislatie.just.ro/Public/DetaliiDocumentAfis/250128.

[21] F. Howarth. (2014, Sep. 2). *The Role of Human Error in Successful Security Attacks*. Securityintelligence [Online]. Available: https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/.

[22] European Union Agency for Network and Information Security. (2017, Nov.). *Cyber Security Culture in organizations*, page 29 [Online]. Available: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations.

[23] S. Sjouwerman. (2021, March). *Stanford Research: 88% of Data Breaches Are Caused by Human Error*. KnowBe4 [Online]. Available: https://blog.knowbe4.com/88-percent-of-data-breaches-are-caused-by-human-error.

[24] Continuitycentral.com. (2021, Jul. 15). *Insider cyber incidents: human error is the top cause of serious data breaches*. Continuitycentral [Online]. Available: https://www.continuitycentral.com/index.php/news/technology/6456-insider-cyber-incidents-human-error-is-the-top-cause-of-serious-data-breaches.

[25] L. Irwin. (2022, July 1st). *Human Error is Responsible for 82% of Data Breaches*. Grcelearning [Online]. Available: https://www.grcelearning.com/blog/human-error-is-responsible-for-85-of-data-breaches.

[26] Data Breach. (2023). *Verizon Data Breach Investigations Report* [Online]. Available: https://www.verizon.com/business/resources/infographics/2023-dbir-infographic.pdf.

[27] Elizabeth Greenberg. (2023, June 16). *Human Error Continues to Receive Most Blame for Cyber Breaches*. Digit News [Online]. Available: https://www.digit.fyi/human-error-continues-to-receive-most-blame-for-cyber-breaches/.

[28] European Security and Defence College, Rehrl, J. (2019). *Handbook on cyber security*. Volume V, 2nd edition, Rehrl, J. (editor), Publications Office, p. 193 [Online]. Available: https://issuu.com/fabry8080/docs/handbook_on_cyber_security__volume_v__2nd_edition_.

[29] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. Indianapolis, IN: Wiley, 2002.

[30] European Security and Defence College, Rehrl, J. (2019). *Handbook on cyber security*. Volume V, 2nd edition, Rehrl, J. (editor), Publications Office, p. 194.

[31] N. Lord. (2018, Sep. 11). *What is Social Engineering? Defining and Avoiding Common Social Engineering Threats*. Digital Guardian [Online]. Available: https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats.

[32] C. Griffiths. (2024, March 1st). *The Latest 2024 Cyber Crime Statistics*. AAG [Online]. Available: https://aag-it.com/the-latest-phishing-statistics/.

[33] ChatGPT, HIX.AI, Chatsonic, Microsoft Bing, YouChat, Claude, Jasper Chat, Perplexity AI, Google Bard, Auto-GPT, Copy.ai, etc.

[34] B. Violino. (2023, Nov. 23). *AI tools such as ChatGPT are generating a mammoth increase in malicious phishing emails*. CNBC Technology Executive Council [Online]. Available: https://www.cnbc.com/2023/11/28/ai-like-chatgpt-is-creating-huge-increase-in-malicious-phishing-email.html.

[35] J. Chapman. (2023, Oct. 23). *Phishing Threat Trends Report*. Egress [Online]. Available: https://pages.egress.com/Whitepaper-

PhishingThreatTrendsReport-10-23_2023-Landing-Page.html.

[36] Cardconnect. (2023, May 19). *Case Study: What We've Learned from the Target Data Breach of 2013* [Online]. Available: https://cardconnect.com/launchpointe/payment-trends/target-data-breach.

[37] S. Oladimeji and S. Michael Kerner. (2023, Nov 3). *SolarWinds hack explained: Everything you need to know*. Tech Target Network [Online]. Available: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

[38] L. Vaas. (2022, Jan. 11). *The FBI warned that attackers are impersonating Health & Human Services and/or Amazon to mail BadUSB-poisoned USB devices to targets in transportation, insurance & defense*. Threat Post [Online]. Available: https://threatpost.com/fin7-mailing-malicious-usb-sticks-ransomware/177541/.

[39] European Union Agency for Network and Information Security. (2022, Sep. 19). *European Cybersecurity Skills Framework* [Online]. Available: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework; https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf.

[40] ICDL. *ICDL Foundation: Shaping Global Standards for Digital Literacy Certification*. [Online]. Available: https://icdleurope.org/about-us/.

Dănuț MAFTEI is currently working for the Romanian National Cyber Security Directorate (DNSC - a governmental body) as a Senior Cyber Security Expert on Policies, Strategies and Cooperation. Meanwhile, he is an EU Expert, working with European Commission/DG NEAR as speaker for TAIEX workshops on cyber issues and digital affairs.

He graduated from the Police Academy in Bucharest and has a PhD degree in Public Order and National Security. With more than 30 years in the government administration, he has been dealing with diplomacy, cyber diplomacy, digital affairs, cybersecurity issues, national / international security, education and international relations. Dănuț MAFTEI has a law enforcement background mixed with diplomatic expertise developed in post conflict countries (EUFOR/BiH and Kosovo – as Head of the Romanian Diplomatic Mission), and EU countries and institutions (Spain, Belgium/Brussels–EU Council). During the RO Presidency of the EU Council (2019), as a diplomat of the RO Permanent Representation to the EU and as the Vice-chair of the Horizontal Party on Cyber Issues / EU Council, he was dealing with diplomacy/foreign affairs, cyber diplomacy, cyber issues, digital affairs and international relations. During 2022-2024, he has been involved in cyber issues, cooperation, international relations and cyber education within DNSC, Bucharest, Romania.