European Agency for Safety and Health at Work

DISCUSSION PAPER

INCORPORATING OCCUPATIONAL SAFETY AND HEALTH IN THE ASSESSMENT OF CYBERSECURITY RISKS

Abstract

This paper discusses a new perspective, investigating the relationship between cybersecurity threats and workers' health and safety. This requires moving past the traditional view of cybersecurity, focused on technical aspects only, and extending the discussion towards the human and social consequences produced by cyberattacks.

Considering the increasing adoption of digital technology in all organisations and the rise of attacks against their computer systems and networks, new emerging risks for workers' health and safety need to be considered. Occupational safety and health (OSH) must deal with new needs and challenges in the years to come.

The cybersecurity scenario

Over the last few years, cybersecurity has become a hot topic for all businesses in all sectors. Cybercrime is becoming more and more sophisticated, and cybercriminals exploit all types of vulnerabilities for their attacks, whether physical, technical or human.

A cyberattack is defined by the Cambridge Dictionary as 'an illegal attempt to harm someone's computer system or the information on it, using the Internet'[1]. More specifically, according to NIST (National Institute of Standards and Technology), a cyberattack is 'an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information'[2].

In a world increasingly digitalised, every business is at risk of cyberattack. In particular 2020 has represented a watershed for both digitalisation and cybersecurity issues. Companies have increased their adoption of organisational approaches based on flexibility and technology to work remotely, mainly because of the COVID-19 pandemic, but this has also represented fertile ground for cybercriminals, to the point where 78% of organisations have experienced an increase in volume of cyberattacks because of the shift towards remote work[3].

Globally, 87% of organisations have been subjected to an attempted exploit of an existing vulnerability, while 71% of security professionals have reported a rise in cybersecurity threats (phishing, malware, ransomware) since the beginning of the coronavirus outbreak[4].

Overall, cybersecurity attacks continue to increase not only in terms of numbers but also in terms of impact (ENISA, 2021a), while countries have different resources and tools to tackle cybersecurity. For example, on the basis of specific factors, like commitment to cybersecurity and legislation, three European countries (Portugal, Lithuania and Slovakia) are classified as having the best cybersecurity index[5].

The expanding threat landscape has determined the urgent need for the European Commission to implement an effective EU cybersecurity strategy for the digital decade[6] to guarantee secure digitalisation, by improving resilience, building the capacity of preventing and responding to cyber incidents, and identifying a coherent international cyber policy. In addition, this strategy highlights the importance of a Cyber Awareness Programme for all EU institutions, bodies and agencies to create an effective cybersecurity culture.

[1] https://dictionary.cambridge.org/dictionary/english/cyberattack
[2] https://csrc.nist.gov/glossary/term/cyber_attack
[3] https://atlasvpn.com/blog/cyberattack-volume-grew-in-78-of-businesses-globally
[4] https://www.checkpoint.com/pages/cyber-security-report-2021/
[5] https://www.eset.com/uk/about/newsroom/blog/european-cybersecurity-index-2021/
[6] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

Current and future threats

It is expected that the cost of cybercrime globally will reach the amount of $10.5 trillion USD annually by 2025[7]. In fact, a variety of actors use cyberspace for malicious purposes and with different motivations, from cybercriminals, essentially moved by financial gain, to cyberterrorists, inspired by political and ideological goals. The area of crime on the Internet is very wide and includes many illegal actions - already known in the physical world - like identity theft, fraud, espionage, intellectual property crime, as well as several forms of online violence (such as stalking or bullying). These actions can rely on the powerful means provided by the digital context, and because of the increasingly interconnected world, cybercrime represents one of the major risks over the next two decades[8].

Cybersecurity threats are a high priority for every organisation and country owing to the variety and severity of consequences: from the loss of valuable information to the paralysis of computer systems and related services as well as serious risks for people's health and safety.

Despite being known for years, some common types of cybersecurity threats (Table 1), like phishing and ransomware continue to increase[9]. In fact, they are very profitable to cybercriminals and the cost of their execution is very low compared to the risk of attackers being caught (Hernandez-Castro et al., 2020). Phishing remains one of the top tactics for security breaches (Verizon, 2021), but the various forms of cyberattacks show the complexity of the cyberthreat landscape. Supply chain attacks, for example, are on the rise and represent a major concern for organisations in the future (ENISA, 2021b)[10].

Table 1: Some of the most common cybersecurity threats[11]

Type	Description
Phishing and spear phishing	Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine. There are different forms of phishing, like spear phishing, a more sophisticated variant of phishing targeted towards a specific individual or organisation.
Malware and ransomware	Malware is a broad term used to describe malicious software, like spyware, ransomware, viruses and worms. Ransomware, for example, is a form of malware that encrypts victims' information and demands payment in return for the decryption key. It is one of the most lucrative types of cyberattacks.
Social engineering	Social engineering is a technique used to deceive and manipulate people to obtain confidential information or gain access to their computer. Phishing is an example of social engineering.
Denial of service (DoS)	This type of attack floods systems, servers, or networks with so much traffic that the system is unable to fulfil legitimate requests. Attackers can also use multiple compromised devices to launch this attack (DDos, distributed-denial-of-service)

[7] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

[8] https://www.weforum.org/agenda/2020/12/3-disruptive-frontier-risks-that-could-strike-by-2040/

[9] https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report

[10] A supply chain is 'the combination of the ecosystem of resources needed to design, manufacture and distribute a product'. In cybersecurity, a supply chain includes hardware and software, cloud or local storage and distribution mechanisms. https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks

[11] These are some of the most common cyber threats reported by ENISA (2020; 2021). For the description of the threats, also see https://www.cisco.com/c/en_in/products/security/common-cyberattacks.html#~types-of-cyber-attacks and https://www.itgovernance.co.uk/cyber-threats

Type	Description
Data breach	A data breach is a security incident in which information is stolen, taken from a system, or used without authorisation.
Cyber espionage	The goal of cyber espionage activities is to steal sensitive or classified data or intellectual property to gain an advantage over a competitive company or government entity.
Disinformation and Misinformation Campaigns	Disinformation consists of creating and sharing false information deliberately to cause harm. Misinformation consists of spreading false or inaccurate information in an accidental way. Both can be preparatory for other attacks (such as social engineering and phishing) and used together with other cybersecurity threats.

The paradox is that on the one hand, innovative technologies can be used for creating new solutions for improving cybersecurity; on the other hand, the same technologies provide further opportunities for cybercriminals themselves. Hence, next to a positive use of Artificial Intelligence (AI), like for intrusion detection and malware identification (Truong et al., 2020), new threats are developed, and traditional threats are reinforced (Brundage et al., 2018). For example, AI technologies can be used for automating social engineering attacks, as well as increasing the effectiveness of malware. Additionally, the proliferation of IoT devices represents further vulnerabilities to handle, since they have weaker processing and storing capabilities, so limiting the security applications for their protection[12].

Specific working situations have increased opportunities for cybercriminals. Remote working, for example, adopted widely during 2020 because of COVID-19, has posed new security challenges for businesses, for example, the creation of more endpoints that can be vulnerable to security breaches and the use of personal devices for work-related activities (BYOD - Bring Your Own Device)[13]. In fact, the comfort of finding everything in one single device is associated with significant security risks, when, for example, imprudent behaviour related to the private use of digital devices is extended to business use (Disterer and Kleiner, 2013). Not to mention that losing a digital device means putting at risk not only personal but also business information. Remote working therefore represents a security challenge for businesses, called upon to revise their corporate policies and invest in robust training for teleworkers (Borkovich and Skovira, 2020).

It is also interesting to observe that workers themselves using wearable devices (such as wi-fi earbuds or smartwatches) can be unconscious vectors for cybercriminals. In fact, wearable technologies present some cybersecurity risks, such as in the case of devices connected to a corporate laptop that could introduce viruses into the company's system, as well as privacy risks caused by unauthorised access (Heembrock, 2015).

Other emerging cybersecurity threats represent further concerns both for individuals and businesses, because of the amplification effects provided by social media. Deep fakes, for example, consist of a digitally altered video or audio file of individuals - often celebrities or politicians - for malicious purposes, like spreading false information and attacking their reputation. However, the concern about these threats goes beyond propaganda and political elections, since they can also affect businesses through market manipulation, brand sabotage, blackmail and digital impersonation of an executive (Westerlund, 2019).

Finally, considering the impressive advancement of technological innovation, it is estimated that quantum computing, which can process information much more efficiently than traditional approaches, could be readily available by 2025[14]. In theory, these computers could break many of today's security

[12] https://www.forbes.com/sites/chuckbrooks/2021/02/07/cybersecurity-threats-the-daunting-challenge-of-securing-the-internet-of-things/

[13] https://www.techrepublic.com/article/how-to-combat-the-security-challenges-of-a-remote-workforce/

[14] https://builtin.com/founders-entrepreneurship/quantum-computing-revolution

encryption schemes, but significant technological advances are required[15] for this technology to be of practical use.

From the scenario just described, it is clear why cyber risks are highly ranked among other global risks (WEF, 2021).

The impact of cyberattacks on OSH

Cyberattacks against businesses and institutions have always been analysed from a technological viewpoint, even though the human factor represents an equally important part of the cybersecurity issue (Corradini et al., 2020). Likewise, looking at the impact of cyberattacks, the focus is primarily on the economic aspects (Cashell et al., 2004; Anderson et al., 2013), and rarely on workers' health and safety. In fact, the impact is mainly measured in terms of tangible costs, like data loss and interruption of business operations, and intangible costs, such as the loss of competitive advantage related to the loss of intellectual property, and damage to reputational brand[16].

Actually, cyberattacks can potentially result in injuries, psychological problems or loss of lives: it is therefore clear that cyber risk assessment and workplace OSH risk assessment cannot be considered as separate activities, but need to be executed together (Izuakor, 2016). Consequentially, businesses should consider a variety of impacts related to cyberthreats and adopt a more comprehensive approach for optimising cybersecurity risk management (Couce-Vieira et al., 2020) as, for example, described in Table 2.

Table 2: The variety of impacts for cybersecurity risk management

Categories	Impacts
Organisation	Economic damages (such as less production related to service unavailability, loss of market share or loss of competitive advantage) Reputation damage (damaged stakeholders' trust) Other economic aspects (such as cyber insurance)
Workers	Physical injuries (such as loss of lives deriving from a failure of a cyber-physical system) Mental health injuries (such as anxiety or frustration) Impact on personal rights (privacy violation deriving from data breaches) Personal economic damage
Other related organisations	Damage due to a disruption of global supply chain interconnections
Environment	Impact on the natural environment (such as land polluted due to a cyber incident)

Adapted from Couce-Vieira et al. 2020

These impacts can be associated with costs measurable in monetary terms, such as the loss of market share, and non-monetary costs, like physical or mental health injuries.

In the following section, the importance of possible physical and psychological impacts on workers' health and safety will be discussed.

[15] https://www.americanscientist.org/article/is-quantum-computing-a-cybersecurity-threat

[16] https://www2.deloitte.com/nz/en/pages/forensic-focus/articles/cyber-security-is-your-organisation-under-threat-of-a-cyber-attack.html

Safety aspects of cybersecurity

The poor consideration of the safety aspects of cybersecurity could be attributed to the perception of cyber risks as external threats, while health and safety issues are handled within organisations[17]. However, the evolution of cyberthreats and the increasing exposure of organisations to cyberattacks calls for the adoption of a holistic approach for managing them effectively, also including the protection of workers' health and safety.

Cyberattacks can put at risk not only the information assets of an organisation, but workers' physical and mental health can also be threatened when hackers attack critical infrastructures[18] or take control of their technological devices. Manipulation of a machine, for example, can physically harm individuals and compromise personal information (Loukas, 2019).

Some examples may clarify this issue. In 2014 in Germany a steel plant was hacked and the attackers managed to shut down the furnace[19]; the risk of transforming a cyberattack into a critical event concerning the workers' safety was very high, because of the nature of materials involved.

In 2017 the US Food and Drug Administration (FDA) recalled approximately 465,000 pacemakers because of security vulnerabilities. The devices were vulnerable to hacking, thus putting patient lives at risk[20].

Cyberattacks on industrial control systems (ICS) that include both cyber and physical elements, are a dangerous threat to human life. Examples include Stuxnet[21], a computer worm created in 2010 for taking control of Iranian centrifuges used for enriching uranium; or Triton Malware[22], that in 2017 involved petrochemical facilities in the Middle East, and fortunately failed. These types of attacks can also produce serious consequences for the environment.

Using equipment remotely in hazardous situations can put workers' safety at risk, like in the case of vehicles or machinery operating out of control because of interrupted wireless signals or attacks by hackers (Steijn et al., 2016).

In the manufacturing sector, when humans and robots cooperate on the production lines, cyberattacks could interrupt physical industrial processes and cause injury to workers (Perales Gómez et al., 2020).

According to Gartner, cyber attackers could weaponise operational technology (OT) and other cyber-physical systems by 2025 to successfully harm or kill humans[23].

Launching a cyberattack against hospitals, hackers can gain access to all patients' and workers' sensitive information; but what can be seriously compromised is the ability for patients to receive proper care and the necessary medical operations (Argaw et al., 2020)[24]. The analysis of the global 'WannaCry' ransomware attack in May 2017 has shown significant negative effects on Britain's National Health Service (Ghafur et al., 2019).

During the COVID-19 pandemic, American hospitals were targeted by a wave of ransomware attacks that interrupted health care in several hospitals, with serious risks for patients' lives[25]. Research focussing on the use of ransomware against healthcare organisations show how these cyberthreats may have life or death consequences (Ponemon, 2021).

[17] https://donesafe.com/2017/06/why-cybersecurity-should-factor-into-every-health-and-safety-plan/

[18] Critical infrastructures are vital for the functioning of a country, given that they include sectors like energy, public health, telecommunication, banking and finance.

[19] https://www.wired.com/2015/01/german-steel-mill-hack-destruction/

[20] https://theconversation.com/three-reasons-why-pacemakers-are-vulnerable-to-hacking-83362

[21] https://spectrum.ieee.org/the-real-story-of-stuxnet

[22] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems/

[23] https://www.thehindubusinessline.com/info-tech/cyber-attackers-could-weaponise-tech-to-kill-humans-by-2025-gartner/article35519872.ece

[24] In 2020, a German hospital fell victim to a cyberattack, making it impossible to accept incoming patients. A woman who was taken there to receive care, died on the way to the next hospital over 30 kilometres away. After the investigation, prosecutors concluded that evidence was insufficient, but it is known that a ransomware attack was responsible for the closure of the hospital's emergency department. https://www.wired.co.uk/article/ransomware-hospital-death-germany

[25] https://www.technologyreview.com/2020/10/29/1011436/a-wave-of-ransomware-hits-us-hospitals-as-coronavirus-spikes/

Social and psychological impacts

Cyberattacks can be associated with social impacts, like a loss of confidence in digital technology, and psychological impacts, like anxiety, anger and depression (Bada and Nurse, 2020). Workers hit by cyberattacks can also end up feeling shamed, guilty, confused or frustrated, especially in the case of leakage of digital information, and the significance of these impacts depends on the environment involved in the cyberattack (Agrafiotis et al., 2018). For example, in a financial institution, where consequences of a data breach are likely to be more severe than in another service provider institution, psychological harm to workers can be higher. In more extreme cases, the consequence of a data leakage may result in the suicide of the affected persons - as the public exposure of the information about them is felt to be so shameful[26] - the psychological burden felt by employees can be very heavy to bear.

Hence, privacy and security are becoming more and more intertwined; while privacy refers to the collection and the use of personal data, security aims at guaranteeing the protection of that data[27]. The General Data Protection Regulation (GDPR), put into effect on May 25, 2018, obligates organisations for data protection and privacy in the EU[28], and in case of data breaches that produce a risk to the rights and freedom of the users, businesses have 72 hours at the latest to notify those affected by the violation.

It is interesting to observe how the violation of privacy can have negative mental health effects on individuals. Privacy, in fact, represents a psychological need strictly related to the development of personal identity (Aboujaoude, 2019).

Research on cybercrime victimisation highlights the negative experiences both for businesses and individuals (for example, Augustina, 2015 and McGuire and Dowling, 2013). Especially when organisations suffer from ransomware attacks, IT teams are affected in terms of damages to professional confidence and high appreciation of skilled staff[29]. Moreover, ransomware attacks are likely to have a greater psychological impact on workersmotions than other security incidents since, when companies pay the ransom, they ‘reward’ the attackers instead of investing money into their personnel[30].

Further considerations can be made about human error, considered the main cause of 90% of cybersecurity breaches[31]. These errors, like opening phishing emails or neglecting password management can expose organisations to serious consequences, such as accidentally installing malicious software onto the company’s network. It can be easily imagined the sense of failure experienced by workers responsible for what happened, which can also inhibit them to report the mistake to their organisation.

With regard to human errors, it is important to consider the psychological factors involved in cybersecurity incidents: 52% of workers are more likely to make mistakes when they are stressed, 43% when they are tired and 26% when they feel burned out[32]. Not to mention that cybersecurity professionals experience a high level of stress or burnout for working to prevent and mitigate cyberattacks[33].

Finally, as a side note, it is important to observe how the cyber dimension also affects violence phenomena. Cyberbullying, for example, is the most widely known form of online harassment (Notar et al., 2013) with the goal of humiliating, persecuting and controlling a person using digital means. Even though this phenomenon is not strictly part of the cybersecurity field, attacks like malware and identity theft can be used to harm people. Online harassment can produce severe psychosomatic, social and mental effects (Dressing et al., 2014; Betts, 2016). Therefore, considering that cyberbullying at work

[26] Ashley Madison, a dating site hacked in July 2015, is a dramatic case in terms of consequences. The data released by hackers included names, passwords, addresses, but also information about customers’ sexual desires. After this data breach, resignations, divorces and suicides occurred. https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked

https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2017/CYB-ET/Pres/8-4%20Waleed%20Hagag_PrivacyVSSecurity.pdf

[28] https://gdpr.eu/tag/gdpr/

[29] https://www.sophos.com/en-us/content/cybersecurity-the-human-challenge.aspx

[30] https://securityintelligence.com/posts/ransomware-response-beyond-money-to-morale/

[31] https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/

[32] https://www.tessian.com/research/the-psychology-of-human-error/

[33] https://news.vmware.com/security/hacking-burnout-for-cybersecurity-awareness-month-2021

(Corradini, 2019; Farley et al., 2021) can put workers' health and safety at risk, this issue should be correctly managed.

Target of cyberattacks

Innovation technology is in every working sector. All organisations - micro, small and medium enterprises (SMEs) as well as large-sized businesses - can be a target for cybercriminals, thus at risk of cyberattacks. Many micro and small businesses do not have the necessary resources for their defence, as evidenced by the fact that 43% of all data breaches involve micro and small businesses (Verizon, 2019).

It is clear that in an increasingly digitalised world, companies are more and more interconnected to each other, thus extending the attack surface.

Looking at the most vulnerable sectors to cyberattacks, according to the IBM Security 2021 Report, Finance and Insurance represented the top attacked industries in 2020 with 23% of attacks, followed by Manufacturing (17.7%), Energy (11.1%), Retail (10.2%), Professional services (8.7%), Government (7.9%), Healthcare (6.6%), Media (5.7%), Transportation (5.1), Education (4.0%).

Observing the evolution of sectors involved in cyberattacks, studies highlight that the healthcare industry is becoming a very attractive target for cybercriminals[34], especially because of the sensitive information stored in medical files (Martin et al., 2017). The COVID-19 pandemic has exacerbated the situation, so that cybercriminals have addressed their attention to intellectual property for vaccine development (Muthuppalaniappan and Stevenson, 2021) and implemented the use of COVID-19-themed phishing emails[35]. However, the healthcare industry has been largely transformed by its fight against the pandemic, and according to future perspectives it must reinforce its security exposure[36].

Even educational organisations are becoming an attractive target for cybercriminals, considering that 44% were hit by ransomware in 2020, and 35% of these paid the ransom to get their data back[37]. The causes are essentially attributed to the limited budgets for cybersecurity and to the large base of users, like students and staff that can increase the exposure to attacks. Moreover, lack of digital awareness among teachers and students requires adopting training programmes for a responsible use of digital technologies (Corradini and Nardelli, 2020).

The current situation regarding cyberattacks is constantly evolving, so it is essential to monitor the updates year by year. In the meantime, a more worrisome picture is emerging. In fact, ransomware actors are testing new extortion methods, leading organisations to cooperate and share information to respond to threat activity[38].

Risk factors for victimisation

Cybercriminals are more interested in attacks on businesses using stolen passwords than committing mass attacks seeking consumer information[39]. However, 330 million adults in 10 countries experienced cybercrime in 2020[40], not to mention that targeting specific workers, for example, through spear phishing, can be an effective strategy to gain access to their organisation.

The risk of falling victim to the different forms of cybercrime depends on both personal and environmental factors (Jansen et al., 2017), and the studies of victims' profiles can help to best comprehend the relationship between cyberattacks and victims' background.

Analysing cybercrime victims across generations, for example, it seems that young adults (under 25 years of age) and the oldest ones (75 and older) are more vulnerable to cyberattacks[41]. Gender represents an important factor in influencing cybersecurity behaviour (Anwar et al., 2017), even though

[34] https://cybersecurityguide.org/industries/healthcare/

[35] https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home

[36] https://www.protiviti.com/US-en/insights/whitepaper-top-risks-2021-and-2030-healthcare-industry-perspective

[37] https://news.sophos.com/en-us/2021/07/13/the-state-of-ransomware-in-education-2021/

[38] https://www.accenture.com/us-en/insights/security/cyber-threat-intelligence-report-2021

[39] https://www.idtheftcenter.org/identity-theft-resource-centers-2020-annual-data-breach-report-reveals-19-percent-decrease-in-breaches/?utm_source=email&utm_medium=TMIEmail012821&utm_campaign=2020DBRReport

[40] https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf

[41] https://risk.lexisnexis.co.uk/about-us/press-room/press-release/20200223-biannual-cybercrime-report

further research in this area - and concerning demographic characteristics - can be very interesting for addressing prevention activities. Some studies have shown that women are more likely to be targeted by phishing attacks (Darwish et al., 2012), while others reveal that women are more concerned about privacy on social networking sites than men (Tifferet, 2019).

Finally, considering the need for reinforcing workplace environments against cybersecurity threats, it appears interesting to analyse how organisational factors, like norms and routines, affect workers' susceptibility to phishing and spear phishing emails (Williams et al., 2018). Such a wide analysis could provide useful insights for enhancing interface design and workers' awareness programmes.

For a comprehensive approach to cybersecurity: the role of awareness

The relationship between cyberthreats and health and safety represent a highly dynamic challenge for organisations, called upon to integrate every necessary measure for an overall corporate approach to cybersecurity[42].

This perspective requires combining safety and security aspects, typically considered as separated concepts, because of different legislative boundaries, interests and practical issues (Boustras and Waring, 2020).

For achieving this goal, the role of awareness of different stakeholders is fundamental, and this should be developed from cybersecurity and OSH viewpoints, strictly interconnected.

For what concerns cybersecurity issues, studies highlight how poor compliance with security and other organisational factors, like insufficient response measures, make organisations vulnerable to cyberattacks (Hart, 2019). In addition, regardless of the variety of working sectors, lack of cybersecurity awareness among workers is responsible for many cybersecurity incidents[43]. Hence, cybersecurity awareness programmes can play an important role in developing an effective cybersecurity culture in organisations (Corradini, 2020) and preventing cyberattacks (Aldawood and Skinner, 2018).

Developing awareness of the possible consequences of cyberattacks in the OSH area requires extending the focus of attention to sources of risk traditionally not considered in relation to workers' health and safety. Positive experiences coming from OSH risk management might also be a great source of inspiration, given that the theme of health and safety in organisations relies on many years of experience, compared to the field of cybersecurity, and many applications and programmes for making safer working environments continue to be implemented successfully. Moreover, managing human failure is considered vital for preventing accidents in the OSH field.

In addition, given that IT security services/departments/experts are not typically familiar with OSH and likewise the OSH community is not familiar with cybersecurity threats, a cooperation between these two areas is essential. For example, a cooperation among OSH, Human Resources, and IT security units within an organisation, where possible, can allow the cyberthreat issue to be viewed from different perspectives and for more efficient, innovative preventive solutions to be implemented.

Raising awareness among stakeholders

Considering what is discussed above, the first step is to sensitise the different stakeholders about the OSH risks associated with cyberthreats so as to lead them to act responsibly.

Awareness-raising programmes can be extremely useful, but to be effective they need to be well-designed and well-tuned to the specific situations, to be suitable for different stakeholders. They should also include a set of tools and methodologies, like campaigns, workshops, conferences, educational materials and other communication activities. Moreover, considering the features of micro-enterprises and SMEs and their limited resources, specific initiatives should be introduced to assist them.

Awareness-raising programmes should involve at least the following internal and external stakeholders:

- **Employers** who are legally responsible for the safety and health of their workers, as well as **management**, are primary actors for their leading role within organisations. Under health and

[42] https://app.croneri.co.uk/feature-articles/health-safety-and-cyber-threats?topic=3682&product=154&section=3511
[43] https://www.techrepublic.com/article/awareness-of-cyberattacks-and-cybersecurity-may-be-lacking-among-workers/

safety law, employers have extensive duties to protect their workers from all work-related risks, and to manage these risks effectively. Since cyberthreats can have an impact on workers' health and safety, they should be explicitly considered in OSH risk prevention and management activities.

- **Workers** must be informed about any risks to their safety and health they might face during their working activities, and cyber risks should be included among them: it is therefore clear that providing information and training to workers on this particular issue is an essential measure for prevention.
- **OSH practitioners** should be involved in awareness initiatives as they generally lack awareness of cybersecurity. They could play a key role in preventing the impacts of cyberattacks on workers' health and safety and should be updated on the evolution of the organisational contexts and the relative risks to cybersecurity.
- **Labour inspectorates**. The new challenges posed by cyberthreats in terms of OSH will probably require new methods and tools for the functions exercised by labour inspectorates. Being aware of the OSH risks associated with cyberthreats is therefore fundamental both for their inspective and preventive role.
- **IT security managers**. They are often not familiar with safety aspects of cybersecurity given that, for the nature of their job, they are essentially focused on network and data security, and on designing and managing an effective IT policy for their organisation. Increasing their awareness on this topic could help to encourage cooperation with OSH experts/ and integrate an additional perspective into defining security rules and practices within organisations.

Given the future extension of cybersecurity-related risks to workplace safety, other types of stakeholders should be aware of the cybersecurity implications for OSH and contribute to prevention strategies. Among these, for example, are experts in Human-Computer Interaction (HCI) and software developers.

HCI is a multidisciplinary field of study, initially focused on the interaction between the users and computers, and now covering many forms of information technology design[44]. Considering that work equipment will be increasingly networked, properly designing HCI interface by experts in this area will be crucial for minimising the impact on cybersecurity and OSH (Korfmacher, 2019).

Similarly, **software developers** can play an important role, considering that a larger and larger share of the working population, whether in house or remotely, carries out their activities by means of software systems. Therefore, it is important to raise software developers' awareness of the impacts of cybersecurity attacks on workers' safety and health to ensure the careful design and realisation of these systems, in terms of their capability to protect against cybersecurity risks, which is going to have a positive impact on the wellbeing of workers, helping them to feel protected against attacks.

In conclusion, a key recommendation is to involve **experts in human behaviour** for designing and implementing cybersecurity awareness programmes. In fact, the success of such initiatives depends on participants' motivations, as well as on the methods and tools used for their deployment. Adequate competences and knowledge on human behaviour are therefore needed.

Finally, cybersecurity is, above all, a human issue. Hence, multidisciplinary teams - combining technical with human and social skills - will be more and more necessary for its effective management.

Next steps

Future studies should focus on the interconnections between the two discussed areas, cybersecurity and OSH. Identifying needs and gaps will help to identify possible risks for workers of cyberattacks, as well as define adequate policies and prevention strategies within organisations. Interesting connections between safety and security have been already discussed in the literature, like the positive relationship among security culture, job satisfaction and compliant security behaviour (Green and D'Arcy, 2010).

Existing research on the relationship between cybersecurity and safety risks is essentially focussed on the healthcare sector (for example, Martin et al., 2017) and on autonomous vehicles (for example,

[44] https://www.interaction-design.org/literature/topics/human-computer-interaction

Taeihagh and Lim, 2019), while more studies are needed to clarify all the possible effects of cyberattacks on workers' health and safety in every working sector.

Moreover, considering that embedded systems will be more and more pervasive in the future, it will be necessary to ensure an adequate integration between security and safety. In fact, these systems could be designed to both respond to security objectives (such as attacks by hackers) and guarantee safety functions, avoiding harms to users (workers). The integration between safety and security is a hot topic in the development of mission-critical systems[45], and international standards can provide a useful support for organisations[46].

Finally, it is possible to suppose that hybrid forms of working - combining home with office work - will be even more widespread in the future, as well as smart working environments based on Internet of Things technologies and cyber-physical systems (Podgórski et al., 2017). Therefore, organisations will need to update their risk assessment to identify any potential hazard for their workers, so as to take adequate measures. For this goal, new methods and tools will have to be implemented.

Concluding remarks

Digital transformation is an unstoppable process, accompanied by several challenges that every country must face. Currently, cybersecurity represents a great concern for companies and institutions of all sizes and sectors, and it will increase in the future.

However, cybersecurity management cannot be reduced to a mere technological protection of systems and information. Since cyberattacks can also affect workers' health and safety, organisations should implement a holistic approach to cybersecurity. Achieving this goal requires **adopting a multidisciplinary vision, integrating technical and social competences** to handle the different implications of cyberthreats.

As for large-sized organisations, the cooperation between IT security and OSH functions is highly recommended for defining an innovative risk assessment process, to protect tangible and intangible assets and, above all, human beings. At the same time, a hot topic is how to implement effective strategies for micro enterprises and SMEs, that often do not have dedicated resources in-house[47], but are exposed to cyberthreat consequences all the same.

The challenge for the future is very hard. To start off on the right foot requires first a robust and wide awareness programme on these topics to prepare employers, workers and the OSH community, as well IT security managers and other relevant actors - like experts in HCI, software developers and experts in human behaviour - for the increasingly digital scenario and the evolution of cyberthreats.

Authors: Isabella Corradini, Scientific director of Themis Research Center (Italy),

Project management: Emmanuelle Brun, Annick Starren, with the contribution of Ana Cayuela, European Agency for Safety and Health at Work (EU-OSHA).

This discussion paper was commissioned by the European Agency for Safety and Health at Work (EU-OSHA). Its contents, including any opinions and/or conclusions expressed, are those of the authors alone and do not necessarily reflect the views of EU-OSHA.

[45] https://insights.sei.cmu.edu/blog/integrating-safety-and-security-engineering-for-mission-critical-systems/

[46] See, for example, ISO/TR 22100-4, Safety of machinery – Relationship with ISO 12100 – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects; IEC TR 63074:2019 'Safety of machinery – Security aspects related to functional safety of safety-related control systems'.

[47] https://www.oecd-ilibrary.org/sites/cb2796c7-en/index.html?itemId=/content/component/cb2796c7-en

References

Aboujaoude, E. (2019). Protecting privacy to protect mental health: The new ethical imperative. *Journal of Medical Ethics*. *45*(9), 604–607.

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S. and Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1).

Aldawood, H. and Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review. In IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE). IEEE, 62–68.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T. and Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.) *The economics of information security and privacy* (265–300). Springer-Verlag.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L. and Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437–443.

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B. and Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making, 20*(146).

Augustina, J. R. (2015). Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology*. *9*(1), 35–54.

Bada, M. and Nurse, J. R. C. (2020). The social and psychological impact of cyber-attacks, psychology. In V. Benson and J. Mcalaney (Eds.), *Emerging cyber threats and cognitive vulnerabilities* (pp. 73–92). Academic Press.

Betts, L. R. (2016). Cyberbullying: Approaches, consequences, and interventions. In J. Binder (Ed.), *Palgrave studies in Cyberpsychology*. Palgrave Macmillan.

Borkovich, D. J. and Skovira, R. J. (2020). Working from home: Cybersecurity in the age of covid-19. *Issues in Information Systems*. *21*(4), 234–236.

Boustras, G. and Waring, A. (2020). Towards a reconceptualization of safety and security, their interactions, and policy requirements in a 21st century context. *Safety Science*, 132.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B. et al. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation.* https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf

Cashell, B., Jackson, W. D., Jickling, M. and Webel, B. (2004). The Economic Impact of Cyber-Attacks. *CRS Report for Congress*.

Corradini, I. (2020). *Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology.* Springer.

Corradini, I. (2019). *Crimini relazionali nell'era digitale. Conoscere per prevenire. Cyber-bullismo-mobbing-stalking.* Themis.

Corradini, I., Nardelli, E. and Ahram, T. (eds.) (2020). *Advances in human factors in cybersecurity*. AHFE 2020. Advances in Intelligent Systems and Computing. Vol 1219, Springer.

Corradini, I. and Nardelli, E. (2020). Developing digital awareness at school: A fundamental step for cybersecurity education. In I. Corradini, E. Nardelli and T. Ahram (Eds.) *Advances in human factors in cybersecurity*. AHFE 2020. Advances in intelligent systems and computing. Vol 1219, Springer.

Couce-Vieira, A., Insua, D. R. and Kosgodagan, A. (2020). Assessing and forecasting cybersecurity impacts. *Decision Analysis. 17*(4), 356–374.

Darwish, A., El Zarka, A. and Aloul, F. (2012). Towards understanding phishing victims' profile. *International Conference on Computer Systems and Industrial Informatics*. 1–5.

Disterer, G. and Kleiner, C. (2013). BYOD - Bring Your Own Device. *HMD.* 50**,** 92–100.

Dressing, H., Bailer, J., Anders, A., Wagner, A. and Gallas, C. (2014). Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Cyberpsychology, Behavior, and Social Networking,* 17: 61–67.

ENISA. (2020). *Threat Landscape 2020*. https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

ENISA. (2021a). Threat Landscape 2021, October 27, 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ENISA (2021b). Threat Landscape for Supply Chain Attacks, July 29, 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Farley, S., Coyne, I. and D'Cruz, P. (2021). Cyberbullying at Work: Understanding the influence of technology. In P. D'Cruz, E. Noronha, G. Notelaers and C. Rayner (Eds.), *Handbooks of workplace bullying, emotional abuse and harassment*. Vol 1, Springer.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. and Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digital Medicine*. *2*(98).

Hamlyn-Harris, J. H. (2017). *Three reasons why pacemakers are vulnerable to hacking.* The Conversation. http://theconversation.com/three-reasons-why-pacemakers-are- vulnerable-to-hacking-83362

Hart, D. V. (2019). Factors influencing the adoption of cybersecurity situational awareness programs. *Isaca Journal*. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/factors-influencing-the-adoption-of-cybersecurity-situational-awareness-programs

Heembrock, M. (2015). The risks of wearable tech in the workplace. *Risk Management Magazine.* https://www.rmmagazine.com/articles/article/2015/02/02/-The-Risks-of-Wearable-Tech-in-the-Workplace-

Hernandez-Castro, J., Cartwright, A. and Cartwright, E. (2020). An economic analysis of ransomware and its welfare consequences. Royal Society Open Science. 7(3), 190023.

Izuakor, C. (2016). Understanding the impact of cyber security risks on safety. ICISSP 2016 - 2nd International Conference on Information Systems Security and Privacy.

Jansen, J., Junger, M., Kort, J., Leukfeldt, R., Veenstra, S., van Wilsem, J. and van der Zee, S. (2017). Victims. In R. Leukfeldt (Ed.), *Research agenda. The human factor in cybercrime and cybersecurity*, Eleven International Publishing.

Kavallieratos, G., Katsikas, S. and Gkioulos, V. (2020). Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—A Comprehensive Survey. *Future Internet*. *12*(4), 65.

Korfmacher, S. (2019). The relevance of cybersecurity for functional safety and HCI. In V. Duffy (Ed.), *Digital human modeling and applications in health, safety, ergonomics and risk management human body and motion HCII 2019 lecture notes in computer science*. 11581. Springer.

Loukas, G. (2019, November). Cyber-physical security threats to Occupational Safety and Health (OSH) in Industry 4.0. https://www.safe-machines-at-work.org/fileadmin/user_upload/pdf/LOUKAS.pdf

Martin, G., Martin, P., Hankin, C., Darzi, A. and Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? British Medical Journal (Clinical research ed.), 358, j3179.

McGuire, M. and Dowling, S. (2013). Cybercrime: A review of the evidence. Summary of key findings and implications (Home Office Research Report, 75). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

Muthuppalaniappan, M., and Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health. *International Journal for Quality in Health Care*, *33*(1).

Notar, C. E., Padgett, S. and Roden, J. (2013). Cyberbullying: A review of the literature. *Universal Journal of Educational Research, 1*(1), 1–9.

Perales Gómez, Á.L., Fernández Maimó, L., Huertas Celdrán, A., García Clemente, F.J., Gil Pérez, M. and Martínez Pérez, G. (2020). SafeMan: A unified framework to manage cybersecurity and safety in manufacturing industry. *Software: Practice and Experience 51*(3), 607–627.

Podgórski, D., Majchrzycka, K., Dąbrowska, A., Gralewicz, G. and Okrasa, M. (2017). Towards a conceptual framework of OSH risk management in smart working environments based on smart PPE, ambient intelligence and the Internet of Things technologies. *International Journal of Occupational Safety and Ergonomics*, *23*(1), 1–20.

Ponemon. (2021). The impact of ransomware on healthcare during covid-19 and beyond. https://www.censinet.com/wp-content/uploads/2021/09/Ponemon-Research-Report-The-Impact-of-Ransomware-on-Healthcare-During-COVID-19-and-Beyond-sept2021-1.pdf

Stacey, N., Ellwood, P., Bradbrook, S., Reynolds, J., Williams, H. and David, L. (2018). *Key trends and drivers of change in information and communication technologies and work location. Foresight on new and emerging risks in OSH.* European Agency for Safety and Health. https://osha.europa.eu/en/publications/foresight-new-and-emerging-occupational-safety-and-health-risks-associated

Steijn, W., van der Vorm, J., Luiijf, E., Gallis, R. and van der Beek, D. (2016, September 6). Emergent risks to workplace safety as a result of IT connections of and between work equipment. *TNO report*.

Taeihagh, A. and Lim, H. S. M. (2019). Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *Transport Reviews*, 39, 103–128.

Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior*, 93: 1–12.

Truong, T. C., Diep, Q. B. and Zelinka, I. (2020). Artificial Intelligence in the Cyber Domain: Offense and Defense. *Symmetry, 12*(3), 410.

Verizon. (2019). 2019 Data breach investigations report. https://www.key4biz.it/wp-content/uploads/2019/05/2019-data-breach-investigations-report.pdf

Verizon. (2021). 2021 Data breach investigations report. https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-data-breach-investigations-report.pdf

WEF. (2021). These are the top cybersecurity challenges of 2021. https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review, 9*(11), 40–53.

Williams, E. J., Hinds, J., and Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120, 1–13.