INCORPORAÇÃO DA SEGURANÇA E SAÚDE NO TRABALHO NA AVALIAÇÃO DOS RISCOS CIBERNÉTICOS

Resumo

O presente documento aborda uma nova perspetiva, investigando a relação entre as ciberameaças e a segurança e saúde dos trabalhadores. Tal implica ir além da visão tradicional da cibersegurança, centrada apenas em aspetos técnicos, e alargar a análise às consequências humanas e sociais resultantes dos ciberataques.

Num contexto de adoção crescente das tecnologias digitais em todas as organizações e de aumento dos ataques contra os seus sistemas e redes informáticos, é necessário ter em conta novos riscos emergentes para a segurança e saúde dos trabalhadores. A segurança e saúde no trabalho (SST) deve dar resposta às novas necessidades e desafios nos próximos anos.

O cenário da cibersegurança

Nos últimos anos, a cibersegurança tornou-se um tema premente para todas as empresas em todos os setores. A cibercriminalidade é cada vez mais sofisticada, e os cibercriminosos exploram todos os tipos de vulnerabilidades nos seus ataques, sejam elas físicas, técnicas ou humanas.

O *Cambridge Dictionary* define um ciberataque como uma tentativa ilegal de utilizar a Internet para provocar danos num determinado sistema informático ou nas informações nele contidas[1]. Mais concretamente, segundo o NIST (Instituto Nacional de Normas e Tecnologia), um ciberataque consiste num ataque, através do ciberespaço, que visa a utilização do ciberespaço por uma empresa com vista a perturbar, desativar, destruir ou, de forma mal intencionada, controlar um ambiente ou infraestrutura de computação, ou destruir a integridade dos dados ou furtar informações controladas[2].

Num mundo cada vez mais digitalizado, todas as empresas estão sujeitas a ciberataques. O ano de 2020, em particular, representou um ponto crítico para as questões da digitalização e da cibersegurança. As empresas reforçaram a adoção de abordagens organizativas baseadas na flexibilidade e na tecnologia para trabalharem à distância, principalmente devido à pandemia da COVID-19, mas tal constituiu também terreno fértil para os cibercriminosos, de tal forma que 78 % das organizações registaram um aumento do volume de ciberataques devido à mudança para o trabalho à distância[3].

A nível mundial, 87 % das organizações foram alvo de tentativas de exploração de uma vulnerabilidade existente, enquanto 71 % dos profissionais da segurança comunicaram um aumento das ciberameaças (*phishing*, *malware*, *ransomware*) desde o início da pandemia devido à COVID-19[4].

Globalmente, os incidentes de cibersegurança continuam a aumentar não apenas em termos numéricos, mas também ao nível do impacto (ENISA, 2021a), num contexto em que os países dispõem de recursos e ferramentas diferentes para abordar a cibersegurança. Por exemplo, tendo por base fatores específicos, como o compromisso com a cibersegurança e a legislação, três países europeus (Portugal, Lituânia e Eslováquia) são classificados como tendo os melhores índices de cibersegurança[5].

Devido ao alargamento do cenário de ameaças, é urgente que a Comissão Europeia aplique uma estratégia eficaz de cibersegurança da UE para a década digital[6], a fim de garantir uma digitalização segura, aumentando a resiliência, reforçando a capacidade para prevenir e responder a ciberincidentes e identificando uma política internacional do ciberespaço coerente. Além disso, esta estratégia salienta

[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

a importância de um programa de cibersensibilização destinado a todas as instituições, organismos e agências da UE, a fim de criar uma cultura de cibersegurança eficaz.

Ameaças atuais e futuras

Prevê-se que, a nível mundial, os custos da cibercriminalidade atinjam 10,5 biliões de USD por ano até 2025[7]. Com efeito, diversos intervenientes utilizam o ciberespaço para fins maliciosos e com diferentes motivações, desde os cibercriminosos, essencialmente motivados pelos ganhos financeiros, aos ciberterroristas, inspirados em objetivos políticos e ideológicos. O domínio da criminalidade na Internet é muito vasto e inclui múltiplas ações ilegais – já conhecidas no mundo físico – como a usurpação de identidade, a fraude, a espionagem ou os crimes contra a propriedade intelectual, bem como várias formas de violência em linha (como a perseguição ou o assédio). Estas ações podem basear-se nos meios poderosos facultados pelo contexto digital e, num mundo cada vez mais interligado, a cibercriminalidade representará um dos maiores riscos durante as próximas duas décadas[8].

As ciberameaças constituem uma grande prioridade para todas as organizações e países devido à variedade e à gravidade das consequências: desde a perda de informações valiosas à paralisação de sistemas informáticos e serviços conexos, bem como riscos graves para a saúde e segurança das pessoas.

Apesar de serem conhecidos há vários anos, alguns tipos comuns de ciberameaças (quadro 1), como o *phishing* (ciberiscagem) e o *rasomware* (software de sequestro), continuam a aumentar[9]. Com efeito, são muito lucrativas para os cibercriminosos e o custo da sua execução é muito reduzido em comparação com o risco de deteção dos autores dos ataques (Hernandez-Castro et al., 2020). A *phishing* continua a ser uma das principais táticas para violações da segurança (Verizon, 2021), mas as diversas formas de ciberataques demonstram a complexidade do cenário de ciberameaças. Os ataques às cadeias de abastecimento, por exemplo, estão a aumentar e constituirão uma grande preocupação para as organizações no futuro (ENISA, 2021b)[10].

Quadro 1: Algumas das ciberameaças mais comuns[11]

Tipo	Descrição
Phishing e *phishing* personalizada	A ciberiscagem consiste na prática de envio de comunicações fraudulentas que parecem ter origem numa fonte idónea, normalmente através de correio eletrónico. Tem como objetivo furtar dados sensíveis, como informações de cartões de crédito e de início de sessão, ou instalar *software* mal-intencionado no dispositivo da vítima. Existem diferentes formas de *phishing* (ciberiscagem), como a *phishing* personalizada, uma variante mais sofisticada que visa uma pessoa ou organização específica.
Malware mal-intencionado e ransomware	O termo *Maleware* «*software* mal-intencionado» é utilizado para descrever *software* malicioso, como *software* espião, *software* de sequestro, vírus e vermes. O Ransomware «*software* de sequestro», por exemplo, é uma forma de *software* mal-intencionado que cifra as informações das vítimas e exige um pagamento em troca da chave de desencriptação. Trata-se de um dos tipos de ciberataque mais lucrativos.

[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] Uma cadeia de abastecimento é a combinação do ecossistema de recursos necessários para conceber, fabricar e distribuir um produto. Na cibersegurança, uma cadeia de abastecimento inclui *hardware* e *software*, armazenamento em nuvem ou local e mecanismos de distribuição. https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks
[11] Trata-se de algumas das ciberameaças mais comuns comunicadas pela ENISA (2020; 2021). Para uma descrição das ameaças, ver também https://www.cisco.com/c/en_in/products/security/common-cyberattacks.html#~types-of-cyber-attacks and https://www.itgovernance.co.uk/cyber-threats

Tipo	Descrição
Engenharia social *Social engineering*	A engenharia social é uma técnica utilizada para enganar e manipular pessoas com vista a obter informações confidenciais ou acesso aos respetivos computadores. A *phishing* é um exemplo de engenharia social.
Negação de serviço *Denial of service* (DoS)	Este tipo de ataque sobrecarrega sistemas, servidores ou redes com um nível de tráfego que torna o sistema incapaz de responder a pedidos legítimos. Por vezes, os autores dos ataques utilizam também vários dispositivos comprometidos para iniciar este ataque (ataques distribuídos de negação de serviço).
Violação de dados *Data breach*	Uma violação de dados consiste num incidente de cibersegurança em que as informações são furtadas, retiradas de um sistema ou utilizadas sem autorização.
Ciberespionagem *Cyber espionage*	As atividades de ciberespionagem têm como objetivo furtar dados sensíveis ou classificados ou propriedade intelectual para adquirir uma vantagem sobre uma empresa concorrente ou uma entidade pública.
Campanhas de desinformação e informação errada	A desinformação consiste na criação e partilha deliberadas de informações falsas para provocar danos. A informação errada consiste na divulgação inadvertida de informações falsas ou inexatas. Ambas podem anteceder outros ataques (nomeadamente de engenharia social e ciberiscagem) e ser utilizadas em conjunto com outras ciberameaças.

É paradoxal que, por um lado, as tecnologias inovadoras possam ser utilizadas para criar novas soluções destinadas a melhorar a cibersegurança mas, por outro, proporcionem mais oportunidades aos próprios cibercriminosos. Por conseguinte, a par de uma utilização positiva da inteligência artificial (IA), nomeadamente para detetar intrusões e identificar *software* mal-intencionado (*malware*) (Truong et al., 2020), estão a ser desenvolvidas novas ameaças e reforçadas ameaças tradicionais (Brundage et al., 2018). Por exemplo, é possível utilizar as tecnologias de IA para automatizar os ataques de engenharia social, bem como para aumentar a eficácia do *software* mal-intencionado. Além disso, a proliferação de dispositivos da Internet das coisas cria mais vulnerabilidades a que é necessário dar resposta, uma vez que as suas capacidades de processamento e de armazenamento são menores, o que limita as aplicações de segurança destinadas a protegê-los[12].

Algumas situações profissionais específicas aumentaram as oportunidades para os cibercriminosos. O trabalho à distância, por exemplo, amplamente adotado durante o ano de 2020 devido à COVID-19, colocou novos desafios de segurança às empresas, como a criação de mais pontos finais que podem ser vulneráveis a violações da segurança e a utilização de dispositivos pessoais para atividades de âmbito profissional («traga o seu próprio dispositivo»)[13]. Com efeito, o conforto de ter tudo num único dispositivo está associado a riscos de segurança significativos, quando, por exemplo, um comportamento imprudente no âmbito do uso privado de dispositivos digitais é replicado na utilização profissional (Disterer e Kleiner, 2013). Além do mais, a perda de um dispositivo digital coloca em risco não apenas as informações pessoais, mas também as informações empresariais. Por conseguinte, o trabalho à distância constitui um desafio de segurança para as empresas, que devem rever as suas políticas empresariais e investir numa formação robusta para os teletrabalhadores (Borkovich e Skovira, 2020).

[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/

É igualmente interessante observar que os próprios trabalhadores que utilizam aparelhos usáveis (como auriculares ligados por Wi-Fi ou relógios inteligentes) podem ser vetores involuntários dos cibercriminosos. Com efeito, as tecnologias usáveis comportam alguns riscos cibernéticos, nomeadamente no caso dos dispositivos ligados a um computador portátil profissional que podem introduzir vírus no sistema da empresa, bem como riscos relacionados com a privacidade resultantes do acesso não autorizado (Heembrock, 2015).

Outras ciberameaças emergentes suscitam preocupações adicionais para as pessoas e empresas, devido aos efeitos de amplificação criados pelas redes sociais. As falsificações profundas, por exemplo, consistem num ficheiro pessoal de vídeo ou de áudio alterado digitalmente – frequentemente de pessoas famosas ou políticos – para fins maliciosos, como a difusão de informações falsas e ataques à sua reputação. Contudo, a preocupação com estas ameaças vai muito para além da propaganda e das eleições políticas, uma vez que podem afetar também as empresas através de manipulação do mercado, sabotagem de marcas, chantagem e usurpação digital de identidade de um executivo (Westerlund, 2019).

Por último, tendo em conta a evolução notável da inovação tecnológica, prevê-se que a computação quântica, que consegue processar informações de forma muito mais eficiente do que as abordagens tradicionais, possa estar facilmente disponível até 2025[14]. Teoricamente, estes computadores podem violar muitos dos atuais esquemas de encriptação de segurança, mas serão necessários progressos tecnológicos significativos[15] para dar uma utilidade prática a esta tecnologia.

O cenário acima descrito deixa claros os motivos pelos quais os riscos cibernéticos ocupam uma posição de destaque entre outros riscos mundiais (FEM, 2021).

O impacto dos ciberataques na SST

Os ciberataques contra empresas e instituições foram sempre analisados do ponto de vista tecnológico, apesar de o fator humano representar uma parte igualmente importante da questão da cibersegurança (Corradini et al., 2020). De igual forma, a análise do impacto dos ciberataques concentra-se sobretudo nos aspetos económicos (Cashell et al., 2004; Anderson et al., 2013) e raramente incide na segurança e saúde dos trabalhadores. Com efeito, o impacto é medido principalmente em termos de custos tangíveis, como a perda de dados e a interrupção da atividade empresarial, e custos intangíveis, como a perda de vantagem concorrencial relacionada com a perda de propriedade intelectual e danos à reputação das marcas[16].

Com efeito, os ciberataques podem resultar em ferimentos, problemas psicológicos ou perda de vidas humanas; por conseguinte, é evidente que a avaliação dos riscos cibernéticos e a avaliação dos riscos de SST não podem ser tratadas como atividades separadas e devem ser realizadas em conjunto (Izuakor, 2016). Consequentemente, as empresas devem ter em conta diversos impactos relacionados com as ciberameaças e adotar uma abordagem mais abrangente para otimizar a gestão dos riscos cibernéticos (Couce-Vieira et al., 2020), como descrito, por exemplo, no quadro 2.

Quadro 2: A diversidade de impactos na gestão dos riscos cibernéticos

Categorias	Impactos
Organização	Prejuízos económicos (como a diminuição da produção devido à indisponibilidade de serviços, à perda de quota de mercado ou à perda de vantagem concorrencial)
	Danos reputacionais (diminuição da confiança das partes interessadas)
	Outros aspetos económicos (como os ciberseguros)

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

Categorias	Impactos
Trabalhadores	Danos físicos (como a perda de vidas humanas devido a uma falha num sistema ciberfísico) Problemas de saúde mental (como a ansiedade ou a frustração) Impacto nos direitos pessoais (violação da vida privada devido a violações de dados) Prejuízos económicos pessoais
Outras organizações conexas	Danos devido a uma perturbação das interligações da cadeia de abastecimento mundial
Ambiente	Impacto no ambiente natural (como a poluição dos solos devido a um ciberincidente

Adaptado de Couce-Vieira et al. 2020

É possível associar estes impactos a custos mensuráveis em termos monetários, como a perda de quota de mercado, e a custos não monetários, como problemas de saúde física ou mental.

A secção seguinte analisa a importância de possíveis impactos físicos e psicológicos na segurança e saúde dos trabalhadores.

Os aspetos de proteção da cibersegurança

A ponderação inadequada dos aspetos de proteção da cibersegurança pode resultar da perceção dos riscos cibernéticos como ameaças externas, em contraste com as questões de segurança e saúde, que são tratadas dentro das organizações[17]. Contudo, a evolução das ciberameaças e a exposição crescente das organizações aos ciberataques exigem a adoção de uma abordagem global que permita gerir eficazmente esses casos, de forma a incluir também a proteção da segurança e saúde dos trabalhadores.

Os ciberataques podem não apenas colocar em risco os ativos de informação de uma organização, mas também ameaçar a saúde física e mental dos trabalhadores, quando os piratas informáticos atacam infraestruturas críticas[18] ou assumem o controlo dos seus dispositivos tecnológicos. A manipulação de uma máquina, por exemplo, pode lesar fisicamente as pessoas e comprometer dados pessoais (Loukas, 2019).

Alguns exemplos poderão clarificar este ponto. Em 2014, na Alemanha, uma unidade siderúrgica foi alvo de um ataque informático, tendo os autores do ataque conseguido desligar o forno[19]; o risco de transformar um ciberataque num acontecimento crítico com impacto na segurança dos trabalhadores era muito elevado, devido à natureza dos materiais em causa.

Em 2017, a Autoridade dos Alimentos e Medicamentos (FDA – Food and Drug Administration) dos EUA recolheu aproximadamente 465 000 estimuladores cardíacos devido a vulnerabilidades de segurança. Os dispositivos eram vulneráveis à pirataria informática, colocando assim em risco as vidas dos doentes[20].

Os ciberataques contra sistemas de controlo industrial (SCI) que incluem elementos cibernéticos e físicos constituem uma ameaça perigosa para a vida humana. É o caso, por exemplo, do Stuxnet[21], um verme criado em 2010 para assumir o controlo de centrifugadoras iranianas utilizadas para

[17] https://donesafe.com/2017/06/why-cybersecurity-should-factor-into-every-health-and-safety-plan/
[18] As infraestruturas críticas são vitais para o funcionamento de um país, uma vez que incluem setores como a energia, a saúde pública, as telecomunicações e os serviços bancários e financeiros.
[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

enriquecer urânio, ou do Triton Malware[22], que, em 2017, visou instalações petroquímicas no Médio Oriente, felizmente sem sucesso. Estes tipos de ataque também podem ter consequências graves para o ambiente.

A utilização de equipamento à distância em situações perigosas pode colocar em risco a segurança dos trabalhadores, nomeadamente no caso de veículos ou máquinas que funcionam sem controlo devido à interrupção de sinais radioelétricos ou a ataques de piratas informáticos (Steijn et al., 2016).

No setor transformador, quando existe cooperação entre seres humanos e robôs nas linhas de produção, os ciberataques podem interromper processos industriais físicos e provocar ferimentos nos trabalhadores (Perales Gómez et al., 2020).

Segundo Gartner, até 2025, os autores de ciberataques serão capazes de utilizar a tecnologia operacional (TO) e outros sistemas ciberfísicos como armas para conseguir ferir ou matar seres humanos[23].

Ao lançarem um ciberataque contra hospitais, os piratas informáticos podem obter acesso a informações sensíveis de todos os doentes e trabalhadores; no entanto, podem sobretudo comprometer seriamente a capacidade de disponibilizar cuidados adequados e as cirurgias necessárias aos doentes (Argaw et al., 2020)[24]. A análise do ataque com o *software* de sequestro «WannaCry» a nível mundial, em maio de 2017, revelou que o mesmo produziu efeitos negativos significativos no Serviço Nacional de Saúde britânico (Ghafur et al., 2019).

Durante a pandemia devido à COVID-19, hospitais norte-americanos foram visados por uma vaga de ataques com *software* de sequestro que interromperam os cuidados de saúde em vários hospitais, colocando seriamente em risco as vidas dos doentes[25]. A investigação centrada na utilização de *software* de sequestro (*ransomware*) contra estabelecimentos de saúde demonstra que estas ciberameaças podem ter consequências de vida ou morte (Ponemon, 2021).

Impactos sociais e psicológicos

Os ciberataques podem estar associados a impactos sociais, como a perda de confiança nas tecnologias digitais, e impactos psicológicos, como a ansiedade, a irritação e a depressão (Bada e Nurse, 2020). Os trabalhadores afetados por ciberataques também podem acabar por se sentir envergonhados, culpados, confusos ou frustrados, em especial quando ocorrem fugas de informações digitais, estando a dimensão desses impactos associada ao ambiente visado pelo ciberataque (Agrafiotis et al., 2018). Por exemplo, numa instituição financeira, em que as consequências de uma violação de dados são tendencialmente mais graves do que em qualquer outra instituição de prestação de serviços, os trabalhadores podem sofrer danos psicológicos mais significativos. Em casos mais extremos, as consequências de uma fuga de dados podem levar as pessoas afetadas a suicidar-se – por se sentirem envergonhadas pela exposição pública das informações a seu respeito[26] – e o ónus psicológico sentido pelos trabalhadores pode ser muito difícil de suportar.

Por conseguinte, a privacidade e a segurança estão cada vez mais interligadas; enquanto a privacidade se refere à recolha e utilização de dados pessoais, a segurança visa garantir a proteção desses dados[27]. O Regulamento Geral sobre a Proteção de Dados (RGPD), entrado em vigor em 25 de maio

[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] Em 2020, um hospital alemão foi alvo de um ciberataque que o impossibilitou de atender doentes. Uma mulher transportada para esse hospital para tratamento faleceu a caminho do hospital mais próximo, situado a mais de 30 quilómetros de distância. Após o inquérito, os procuradores concluíram que as provas eram insuficientes, mas é sabido que foi um ataque com *software* de sequestro (ransomware) o responsável pelo encerramento do serviço de urgência do hospital. 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/

[26] «Ashley Madison», um sítio de contactos românticos alvo de pirataria informática em junho de 2015, é um caso dramático devido às suas consequências. Os dados divulgados pelos piratas informáticos incluíam nomes, palavras-passe e endereços, mas também informações sobre os desejos sexuais dos clientes. Esta violação de dados conduziu a demissões, divórcios e suicídios.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

de 2018, obriga as organizações a assegurarem a proteção de dados e a privacidade na UE[28] e, nos casos de violações de dados que implicam riscos para os direitos e liberdades dos utilizadores, as empresas têm 72 horas, no máximo, para notificar os afetados pela violação em causa.

É interessante observar a forma como a violação da vida privada pode ter efeitos negativos na saúde mental das pessoas. Com efeito, a privacidade representa uma necessidade psicológica estreitamente associada ao desenvolvimento da identidade pessoal (Aboujaoude, 2019).

A investigação sobre a vitimização na cibercriminalidade realça as experiências negativas tanto das empresas como das pessoas (por exemplo, Augustina, 2015, e McGuire e Dowling, 2013). Principalmente quando as organizações são alvo de ataques com *software* de sequestro (*ransomware*), as equipas informáticas enfrentam uma deterioração da confiança profissional e da elevada valorização da mão de obra qualificada[29]. Além disso, os ataques com *software* de sequestro[30] têm tendencialmente um maior impacto psicológico nos trabalhadores do que outros incidentes de cibersegurança, já que, quando as empresas pagam o resgate, «premeiam» os autores do ataque em vez de investirem financeiramente no seu pessoal.

É possível aprofundar as considerações sobre o erro humano, que é considerado como a principal causa de 90 % das violações da cibersegurança[31]. Estes erros, tais como abrir mensagens de correio eletrónico de ciberiscagem (*phishing*)ou negligenciar a gestão das palavras-passe, pode expor as organizações a consequências graves, por exemplo a instalação inadvertida de *software* malicioso na rede de uma empresa. É fácil imaginar a sensação de falhanço dos trabalhadores responsáveis pelo sucedido, que também os pode inibir de comunicar o erro à organização a que pertencem.

No que diz respeito aos erros humanos, é importante ter em conta os fatores psicológicos associados a incidentes de cibersegurança: 52 % dos trabalhadores são mais suscetíveis a erros quando estão sob tensão, 43 % quando se sentem cansados e 26 % quando se sentem esgotados[32]. Além do mais, os profissionais da cibersegurança apresentam um elevado nível de tensão ou esgotamento pelo facto de lhes caber evitar e atenuar ciberataques[33]..

Por último, a título complementar, é importante observar a forma como a dimensão cibernética afeta também os fenómenos de violência. O ciberassédio, por exemplo, é a forma mais conhecida de assédio em linha (Notar et al., 2013), tendo como objetivo humilhar, perseguir e controlar uma pessoa utilizando meios digitais. Embora este fenómeno não se insira apenas no domínio da cibersegurança, ataques como o *software* mal-intencionado (*malware*) e a usurpação de identidade podem ser utilizados para lesar pessoas. O assédio em linha pode produzir efeitos psicossomáticos, sociais e mentais graves (Dressing et al., 2014; Betts, 2016). Por conseguinte, tendo em conta que o ciberassédio no trabalho (Corradini, 2019; Farley et al., 2021) pode colocar em risco a segurança e saúde dos trabalhadores, é importante gerir corretamente esta questão.

Alvos dos ciberataques

As tecnologias inovadoras estão presentes em todos os setores do trabalho. Todas as organizações – tanto as microempresas e pequenas e médias empresas (PME) como as empresas de grande dimensão – podem ser alvos dos cibercriminosos e, por conseguinte, enfrentam o risco de ciberataques. Muitas micro e pequenas empresas não dispõem dos recursos necessários para se defenderem, como revela o facto de 43 % de todas as violações de dados estarem ligados a empresas dessa dimensão (Verizon, 2019).

É notório que, num mundo cada vez mais digitalizado, as empresas estão cada vez mais interligadas, o que aumenta a superfície de ataque.

Analisando os setores mais vulneráveis a ciberataques, de acordo com o relatório da IBM sobre a segurança relativo a 2021, os setores financeiro e dos seguros foram os mais atacados em 2020, com 23 % dos ataques, seguindo-se o setor transformador (17,7 %), a energia (11,1 %), o comércio

[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

retalhista (10,2 %), os serviços profissionais (8,7 %), os serviços públicos (7,9 %), os cuidados de saúde (6,6 %), os meios de comunicação social (5,7 %), os transportes (5,1 %) e a educação (4,0 %) (IBM Security, 2021).

Observando a evolução dos setores envolvidos em ciberataques, os estudos salientam que o setor da saúde se está a tornar um alvo muito atrativo para os cibercriminosos[34], em especial devido às informações sensíveis constantes dos processos clínicos (Martin et al., 2017). A pandemia devido à COVID-19 agravou a situação, na medida em que os cibercriminosos voltaram a sua atenção para a propriedade intelectual relacionada com o desenvolvimento das vacinas (Muthuppalaniappan e Stevenson, 2021) e introduziram a utilização de mensagens de correio eletrónico de ciberiscagem (*phishing*) sobre o tema da COVID-19[35]. Contudo, o setor da saúde sofreu alterações significativas devido ao combate à pandemia e as perspetivas para o futuro indicam que será obrigado a aumentar a sua exposição a riscos de segurança[36].

Até os estabelecimentos de ensino se estão a tornar alvos atrativos para os cibercriminosos, tendo em conta que, em 2020, 44 % foram atingidos por *software* de sequestro (*ransomware*) e, destes, 35 % pagaram o resgate para recuperar os seus dados[37]. As causas são imputáveis essencialmente aos orçamentos limitados para a cibersegurança e à grande base de utilizadores, nomeadamente estudantes e pessoal, que pode aumentar a exposição a ataques. Além disso, a falta de sensibilização digital dos professores e dos alunos exige a adoção de programas de formação para uma utilização responsável das tecnologias digitais (Corradini e Nardelli, 2020).

A atual situação em matéria de ciberataques está em constante evolução, pelo que é essencial acompanhar as atualizações ano a ano. Entretanto, o cenário está a tornar-se mais preocupante. Com efeito, os responsáveis pelo *software* de sequestro (*ransomware*) estão a testar novos métodos de extorsão, levando as organizações a cooperar e a partilhar informações em resposta a atividades ameaçadoras[38].

Fatores de risco na vitimização

Os cibercriminosos estão mais interessados em ataques a empresas com recurso a palavras-passe furtadas do que em ataques maciços em busca de informações dos consumidores[39]. Contudo, 330 milhões de adultos, em 10 países, foram alvo da cibercriminalidade em 2020[40], além de que os ataques contra trabalhadores específicos, por exemplo através da ciberiscagem (*phishing*) personalizada, pode ser uma estratégia eficaz para obter acesso à organização a que pertencem.

O risco de ser vítima das diferentes formas de cibercriminalidade depende de fatores pessoais e ambientais (Jansen et al., 2017), e os estudos dos perfis das vítimas podem ajudar a compreender melhor a relação entre os ciberataques e os contextos das vítimas.

Por exemplo, a análise geracional das vítimas da cibercriminalidade sugere que os jovens adultos (com idade inferior a 25 anos) e as pessoas mais velhas (com idade igual ou superior a 75 anos) são mais vulneráveis a ciberataques[41]. O género constitui um fator importante do comportamento em matéria de cibersegurança (Anwar et al., 2017), embora outros estudos neste domínio – relacionados também com as características demográficas – possam ser muito interessantes para abordar as atividades de prevenção. Alguns estudos demonstraram que as mulheres são alvos mais prováveis dos ataques de ciberiscagem (*phishing*) (Darwish et al., 2012), enquanto outros revelam que as mulheres estão mais preocupadas do que os homens com a privacidade nas redes sociais (Tifferet, 2019).

Por último, tendo em conta a necessidade de reforçar os ambientes de trabalho contra as ciberameaças, afigura-se interessante analisar a forma como os fatores organizacionais, por exemplo as normas e as rotinas, afetam a suscetibilidade dos trabalhadores à ciberiscagem (*phishing*) e às

[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

mensagens de correio eletrónico de ciberiscagem (*phishing*) personalizada (Williams et al., 2018). Esta análise abrangente poderia proporcionar informações úteis para reforçar a conceção das interfaces e os programas de sensibilização dos trabalhadores.

Rumo a uma abordagem global da cibersegurança: o papel da sensibilização

A relação entre as ciberameaças e a segurança e saúde no trabalho representa um desafio bastante dinâmico para as organizações, que devem integrar todas as medidas necessárias para uma abordagem empresarial global da cibersegurança[42].

Esta perspetiva exige a combinação de aspetos de proteção e segurança, geralmente consideradas como conceitos separados, devido às suas diferenças em matéria de limites da legislação, interesses e questões práticas (Boustras e Waring, 2020).

A sensibilização das diferentes partes interessadas é fundamental para cumprir este objetivo e deve ser desenvolvida dos pontos de vista da cibersegurança e da SST, com uma estreita ligação entre ambas.

No que diz respeito às questões de cibersegurança, os estudos salientam a forma como um cumprimento deficiente de fatores de segurança e outros fatores organizacionais, nomeadamente medidas de resposta insuficientes, tornam as organizações vulneráveis a ciberataques (Hart, 2019). Além disso, independentemente da variedade dos setores do trabalho, a falta de sensibilização para a cibersegurança entre os trabalhadores é responsável por muitos incidentes de cibersegurança[43]. Por conseguinte, os programas de sensibilização para a cibersegurança podem desempenhar um papel importante no desenvolvimento de uma cultura de cibersegurança eficaz nas organizações (Corradini, 2020) e na prevenção de ciberataques (Aldawood e Skinner, 2018).

O reforço da sensibilização para as possíveis consequências dos ciberataques no domínio da SST exige que se concentrem atenções também nas fontes de risco que tradicionalmente não são associadas à segurança e saúde dos trabalhadores. Experiências positivas resultantes da gestão dos riscos de SST também poderão constituir uma excelente fonte de inspiração, uma vez que o tema da segurança e saúde nas organizações se baseia em muitos anos de experiência, ao contrário do domínio da cibersegurança, e que continuam a ser implementadas com êxito muitas aplicações e programas para aumentar a segurança dos ambientes de trabalho. Acresce que a gestão do erro humano é considerada fundamental para prevenir acidentes no domínio da SST.

Além disso, uma vez que, geralmente, os serviços/departamentos/peritos de segurança informática não estão familiarizados com a SST e, de igual modo, a comunidade da SST não conhece bem as ciberameaças, é essencial que exista cooperação entre estes dois domínios. Por exemplo, a cooperação entre as unidades de SST, recursos humanos e segurança informática numa organização, sempre que possível, pode permitir analisar a questão das ciberameaças de diferentes pontos de vista e aplicar soluções preventivas mais eficientes e inovadoras.

Aumentar a sensibilização entre as partes interessadas

Tendo em conta o que precede, o primeiro passo consiste em sensibilizar as diferentes partes interessadas para os riscos de SST associados às ciberameaças, a fim de as incentivar a agir de forma responsável.

Os programas de sensibilização podem ser extremamente úteis mas, para serem eficazes, devem ser bem concebidos e ajustados a situações específicas para serem adequados a diferentes partes interessadas. Devem incluir também um conjunto de ferramentas e metodologias, como campanhas, ateliês, conferências, materiais educativos e outras atividades de comunicação. Além disso, tendo em conta as características das microempresas e das PME e os seus recursos limitados, é importante introduzir iniciativas específicas para as apoiar.

Os programas de sensibilização devem incluir pelo menos as seguintes partes interessadas internas e externas:

[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/

- Os **empregadores**, que são legalmente responsáveis pela segurança e saúde dos seus trabalhadores, bem como os **gestores**, são intervenientes essenciais devido ao seu papel de liderança nas organizações. Em conformidade com a legislação em matéria de segurança e saúde, os empregadores têm amplos deveres de proteção dos seus trabalhadores contra todos os riscos profissionais e de gestão eficaz dos mesmos. Uma vez que podem ter impacto na segurança e saúde dos trabalhadores, as ciberameaças devem ser explicitamente consideradas nas atividades de prevenção e gestão dos riscos de SST.
- Os **trabalhadores** devem ser informados sobre quaisquer riscos para a segurança e saúde a que possam estar sujeitos durante as suas atividades profissionais, incluindo os ciber-riscos: por conseguinte, é evidente que a prestação de informações e formação aos trabalhadores sobre este tema específico constitui uma medida de prevenção essencial.
- Os **profissionais de SST** devem ser envolvidos em iniciativas de sensibilização, já que, de um modo geral, não estão suficientemente sensibilizados para a cibersegurança. Podem desempenhar um papel fundamental na prevenção dos impactos dos ciberataques na segurança e saúde dos trabalhadores e devem obter atualizações sobre a evolução dos contextos organizacionais e dos riscos relativos para a cibersegurança.
- **Serviços de inspeção do trabalho**. Os novos desafios colocados pelas ciberameaças no domínio da SST exigirão provavelmente novos métodos e ferramentas para as funções exercidas pelos serviços de inspeção do trabalho. Por conseguinte, a sensibilização para os riscos de SST associados às ciberameaças é fundamental para o seu papel de inspeção e de prevenção.
- **Gestores de segurança informática**. Muitas vezes, estes intervenientes não estão familiarizados com os aspetos de proteção da cibersegurança, uma vez que, devido à natureza do seu trabalho, se concentram essencialmente na segurança das redes e dos dados e não na conceção e gestão de uma política informática eficaz para a sua organização. O aumento da sua sensibilização para este tema poderia ajudar a incentivar a cooperação com peritos em SST e a integrar uma perspetiva adicional na definição das regras e práticas de segurança nas organizações.

Tendo em conta que os riscos relacionados com a cibersegurança abrangerão, no futuro, a segurança no local de trabalho, outros tipos de partes interessadas deverão estar cientes das implicações da cibersegurança para a SST e contribuir para estratégias de prevenção. É o caso, por exemplo, dos peritos em interação entre humanos e computadores (HCI - Human-Computer Interaction) e dos criadores de *software*.

A **HCI** é uma área de estudo multidisciplinar, centrada inicialmente na interação entre os utilizadores e os computadores, que abrange agora muitas formas de conceção das tecnologias da informação[44]. Tendo em conta que o equipamento de trabalho estará cada vez mais ligado em rede, uma conceção adequada da interface HCI por peritos neste domínio será fundamental para minimizar o impacto na cibersegurança e na SST (Korfmacher, 2019).

Os **criadores de *software*** também podem desempenhar um papel importante, já que uma percentagem cada vez maior da população ativa, em casa ou à distância, exerce as suas atividades com recurso a sistemas de *software*. Por conseguinte, é importante aumentar a sensibilização dos criadores de *software* para os impactos dos incidentes de cibersegurança na segurança e saúde dos trabalhadores, a fim de assegurar uma conceção e aplicação cuidadosas destes sistemas, no que diz respeito à sua capacidade de proteção contra riscos cibernéticos, que terão um impacto positivo no bem-estar dos trabalhadores, ajudando-os a sentir-se protegidos contra ataques.

Em conclusão, uma recomendação essencial consiste em envolver **peritos em comportamento humano** na conceção e aplicação dos programas de sensibilização para a cibersegurança. Com efeito, o êxito dessas iniciativas está dependente das motivações dos participantes, bem como dos métodos utilizados na sua implantação. Por conseguinte, são necessárias competências e conhecimentos adequados sobre o comportamento humano.

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

Por último, a cibersegurança é, acima de tudo, uma questão humana. Como tal, serão cada vez mais necessárias equipas multidisciplinares – que combinem competências humanas e sociais – para a gerir eficazmente.

Próximas etapas

Estudos futuros devem concentrar-se nas interligações entre os dois domínios analisados, ou seja, a cibersegurança e a SST. A identificação das necessidades e das lacunas ajudará a identificar possíveis riscos dos ciberataques para os trabalhadores, bem como a definir políticas e estratégias de prevenção adequadas dentro das organizações. A literatura existente já analisou ligações interessantes entre a proteção e a segurança, como a relação positiva entre a cultura de segurança, a satisfação profissional e um comportamento conforme em matéria de segurança (Green e D'Arcy, 2010).

Os estudos existentes sobre a relação entre a cibersegurança e os riscos de segurança concentram-se essencialmente no setor da saúde (por exemplo, Martin et al., 2017) e nos veículos autónomos (por exemplo, Taeihagh e Lim, 2019), sendo necessários mais estudos para clarificar todos os possíveis efeitos dos ciberataques na segurança e saúde dos trabalhadores em todos os setores do trabalho.

Além disso, uma vez que os sistemas incorporados serão cada vez mais generalizados no futuro, será necessário assegurar uma integração adequada entre segurança e proteção. Com efeito, estes sistemas poderão ser concebidos para, simultaneamente, dar resposta aos objetivos de segurança (como os ataques de piratas informáticos) e garantir funções de segurança, evitando danos para os utilizadores (os trabalhadores). A integração entre proteção e segurança é um tema premente no desenvolvimento de sistemas de missão crítica[45], e as normas internacionais podem constituir um apoio útil para as organizações[46].

Por último, é possível antever que as formas de trabalho híbridas – que combinam o trabalho no domicílio com o trabalho em escritório – serão ainda mais generalizadas no futuro, da mesma forma que os ambientes de trabalho inteligentes baseados em tecnologias da Internet das coisas e em sistemas ciberfísicos (Podgórski et al., 2017). Por conseguinte, as organizações terão de atualizar a sua avaliação dos riscos para identificar qualquer potencial perigo para os seus trabalhadores e, consequentemente, tomar medidas adequadas. Para o efeito, será necessário aplicar novos métodos e ferramentas.

Observações finais

A transformação digital é um processo imparável que coloca vários desafios a todos os países. Atualmente, a cibersegurança representa uma grande preocupação para empresas e instituições de todas as dimensões e de todos os setores, que aumentará no futuro.

No entanto, a gestão da cibersegurança não se pode resumir apenas à proteção tecnológica de sistemas e informações. Uma vez que os ciberataques também podem afetar a segurança e saúde dos trabalhadores, as organizações devem aplicar uma abordagem global da cibersegurança. Para cumprir este objetivo, é necessário **adotar uma visão multidisciplinar, que integre competências técnicas e sociais**, para fazer face às diferentes implicações das ciberameaças.

No que diz respeito às organizações de grande dimensão, é altamente recomendável uma cooperação entre as funções de segurança informática e de SST, a fim de definir um processo inovador de gestão dos riscos, protegendo ativos tangíveis e intangíveis e, acima de tudo, os seres humanos. Simultaneamente, é urgente perceber como aplicar estratégias eficazes para as microempresas e as PME, as quais, muitas vezes, não dispõem de recursos internos específicos[47] mas estão igualmente expostas às consequências das ciberameaças.

Este desafio futuro é muito complexo. Para começar da melhor forma, é necessário definir previamente um programa de sensibilização robusto e alargado sobre estes temas, a fim de preparar os empregadores, os trabalhadores e a comunidade de SST, bem como os gestores da segurança informática e outros intervenientes relevantes – nomeadamente peritos em interação entre humanos e

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

computadores (HCI), criadores de *software* e peritos em comportamento humano – para o cenário cada vez mais digital e para a evolução das ciberameaças.

Autora: Isabella Corradini, diretora científica do Centro de Investigação Themis (Itália).

Gestão do projeto: Emmanuelle Brun, Annick Starren, com o contributo de Ana Cayuela, Agência Europeia para a Segurança e Saúde no Trabalho (EU-OSHA).

Referências

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. e 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. e 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. e 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. e 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. e 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. e Nurse, J. R. C. (2020). «The social and psychological impact of cyber-attacks, psychology». *In* V. Benson e J. Mcalaney (ed.), *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. e Skovira, R. J. (2020). «Working from home: Cybersecurity in the age of covid-19». *Issues in Information Systems*. *21*(4), 234-236.

Boustras, G. e 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. e 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. e Ahram, T. (ed.) (2020). *Advances in human factors in cybersecurity*. AHFE 2020. Advances in Intelligent Systems and Computing. Vol. 1219, Springer.

Corradini, I. e Nardelli, E. (2020). «Developing digital awareness at school: A fundamental step for cybersecurity education». *In* I. Corradini, E. Nardelli e T. Ahram (ed.) *Advances in human factors in cybersecurity*. AHFE 2020. Advances in Intelligent Systems and Computing. Vol. 1219, Springer.

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

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

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

Dressing, H., Bailer, J., Anders, A., Wagner, A. e 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*, 27 de outubro de 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

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

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

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. e 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. e Cartwright, E. (2020). «An economic analysis of ransomware and its welfare consequences». *Royal Society Open Science*. 7(3), 190023.

IBM Security, X-Force Threat Intelligence Index 2021 https://www.ibm.com/downloads/cas/M1X3B7QG

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. e 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. e 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. (novembro de 2019). «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. e Kinross, J. (2017). «Cybersecurity and healthcare: How safe are we?» *British Medical Journal (Clinical Research Edition)*, 358, j3179.

McGuire, M. e 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., e 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. e 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. e 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. e 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. e 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.* Agência Europeia para a Segurança e Saúde no Trabalho. 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. e van der Beek, D. (6 de setembro de 2016). «Emergent risks to workplace safety as a result of IT connections of and between work equipment». *TNO report*.

Taeihagh, A. e 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. e 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., e Joinson, A. N. (2018). «Exploring susceptibility to phishing in the workplace». *International Journal of Human-Computer Studies*, 120, 1-13.