The U.S. Cyber Threat Landscape

Elie Alhajjar and Kevin Lee
Army Cyber Institute, West Point, USA
elie.alhajjar@westpoint.edu
kevin.lee@westpoint.edu

Abstract: Cybersecurity is concerned with protecting information, hardware, and software on the internet from unauthorized use, intrusions, sabotage, and natural disasters. It is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage, or unauthorized access. The numerous ways in which computer systems and data can be compromised and the dramatic increase in cybercrimes have made cybersecurity a growing field. One of the most problematic elements of cybersecurity is the quick and constant evolving nature of security risks in critical infrastructure and major businesses all around the world. In this paper, we sketch a general frame for the cyber threat landscape in the United States of America by focusing on five major categories: ransomware, social engineering, third party software, deep fakes, and insider threats. We elaborate on each of these pillars by providing case studies from the past decade, as well as discussing ways to move forward.

Keywords: cyber threat, ransomware, insider threat, malware, social engineering, deepfakes

1. Introduction

Advancements in information technology (IT) have raised concerns about the risks to data associated with weak IT security, including vulnerability to viruses, malware, attacks and compromise of network systems and services. Inadequate IT security may result in compromised confidentiality, integrity, and availability of the data due to unauthorized access. Nowadays, a general rule of thumb is the following: All networks are vulnerable to cybersecurity threats!

According to the Practical Law Company (Farhat, McCarthy and Raysman, 2011), a cyberattack is an attack initiated from a computer against a website, computer system or individual computer that compromises the confidentiality, integrity or availability of the computer or information stored on it. Cyberattacks may take different forms, while having many objectives such as gaining unauthorized access to a computer system or its data, disrupting normal activities including the take down of entire web sites, installing viruses or malicious code on a computer system, changing the characteristics of a computer system's hardware, firmware or software without the owner's knowledge, instruction, or consent, inappropriately using computer systems by current and/or former employees, etc.

A cyber threat is an activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains. Cyber threat actors are states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, and technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks. The globalized nature of the Internet allows these threat actors to be physically located anywhere in the world and still affect the security of information systems. Cyber threat actors can be categorized by their motivations and, to a degree, by their sophistication. Threat actors value access to devices, processing power, computing resources, and information for different reasons. In general, each type of cyber threat actor has a primary motivation.

Cyber threat actors are not equal in terms of capability and sophistication, and have a range of resources, training, and support for their activities. Cyber threat actors may operate on their own or as part of a larger organization. In some cases, even sophisticated actors use less sophisticated and readily available tools and techniques because these can still be effective for a given task and make it difficult for defenders to attribute the activity. Nation-states are frequently the most sophisticated threat actors, with dedicated resources and personnel, and extensive planning and coordination. Cybercriminals are generally understood to have moderate sophistication in comparison to nation-states. Nonetheless, they still have planning and support functions in addition to specialized technical capabilities that affect a large number of victims. Hacktivists, terrorist groups, and thrill-seekers are typically at the lowest level of sophistication as they often rely on widely available tools that require little technical skill to deploy. Their actions, more often than not, have no lasting effect on their targets beyond reputation. Finally, insider threats are individuals working within their organization who are

particularly dangerous because of their access to internal networks that are protected by security perimeters. Access is a key component for malicious threat actors and having privileged access eliminates the need to employ other remote means. Insider threats may be associated with any of the other listed types of threat actors but can also include disgruntled employees with motive.

Of particular interest is the notion of cyber-terrorism (Denning, 2000): "Cyber-terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber-terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber-terrorism, depending on their impact." Terrorists' activities via cyberspace include creating websites/blogs, communication via email, discussion via chat rooms, e-transactions (e-commerce/ e-banking), using search engines to collect data and information, phishing/ hacking, viruses, malicious code, etc. (Alhajjar, Fameli and Warren, 2020).

There are various threats to an organization's information system; understanding the vast array of threats is the first step in ensuring adequate protection of sensitive data. A holistic approach to data security begins with understanding the network, its architecture, user population, and mission requirements. In this paper, we aim at providing a "big picture" view of the cyber threat landscape in the United States of America. To this end, the current paper is organized as follows. After this brief introduction, we give an overview of the main five cybersecurity threats, namely ransomware, social engineering, malware, deep fakes, and insider threats in sections 2-6, respectively. We discuss many case studies and highlight their details. We conclude our work in section 7 and suggest some ways to mitigate such threats in the future.

2. Ransomware

Ransomware is a type of malware that involves an attacker locking the victim's computer system files typically through encryption and demanding a payment to decrypt and unlock them. It is a rising threat that utilizes malicious software that prevents a user from accessing computer files, systems, or networks demanding a ransom for their return. If the ransom is not paid, the victim's data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim's data or to release it to the public.

Generally speaking, one can distinguish ransomware attacks into three categories (Loman 2019). First, cryptoworm is a standalone ransomware that replicates itself to other computers for maximum reach and impact. Second, Ransomware-as-a-Service (RaaS) is sold on the dark web as a distribution kit to anyone who can afford it. Such RaaS packages allow people with little technical skill to attack with relative ease. They are typically deployed via malicious spam emails, via exploit kits as a drive-by download, or semi-manually by automated active adversaries. Third, automated active adversary is a ransomware attack deployed by actors who use tools to automatically scan the internet for IT systems with weak protection. When such systems are found, the attackers establish a foothold and from there carefully plan the ransomware attack for maximum damage.

Although cyber criminals use a variety of techniques to infect victims with ransomware, the most common means of infection are email phishing campaigns, Remote Desktop Protocol (RDP), and software vulnerabilities. In the first case, the cybercriminal sends an email containing a malicious file or link, which deploys malware when clicked by a recipient. Cyber criminals historically have used generic, broad-based spamming strategies to deploy their malware, though recent ransomware campaigns have been more targeted and sophisticated. Criminals may also compromise a victim's email account by using precursor malware, which enables the cybercriminal to use a victim's email account to further spread the infection. In the second case, RDP is a proprietary network protocol that allows individuals to control the resources and data of a computer over the internet. Cybercriminals have used both brute-force methods, a technique using trial-and-error to obtain user credentials, and credentials purchased on dark web market. Once they have RDP access, criminals can deploy a range of ransomware attacks to victim systems. In the third case, cybercriminals can take advantage of security weaknesses in widely used software programs to gain control of victim systems and deploy ransomware.

In May of 2021, Colonial Pipeline announced that it had fallen victim to a devastating ransomware attack that shut down operations and cut off fuel supplies to millions, causing massive economic disruption across the

Eastern United States. The FBI confirmed the attacks were executed by the DarkSide ransomware gang, a relatively new threat actor that Cybereason has been tracking since August 2020. They have a mature Ransomware as a Service (RaaS) business model and affiliate program. The group has a phone number and even a help desk to facilitate negotiations with and collect information about its victims, not just technical information regarding their environment but also more general details relating to the company itself like the organization's size and estimated revenue. DarkSide follows the double extortion trend, where the threat actors first exfiltrates sensitive information stored on a victim's systems before launching the encryption routine. After the ransomware encrypts the target's data and issues the ransom demand for payment in exchange for the decryption key, the threat actors make the additional threat of publishing the exfiltrated data online should the target refuse to make the ransom payment.

On or about 18 Feb 2018, a threat actor gained access to the Colorado Department of Transportation (CDOT) network via a virtual server and installed the SamSam ransomware malware variant. Two days later, the ransomware became active and infected approximately 150 servers and 2000 workstations. The Remote Desktop protocol is how this attack was initiated: the attacker discovered the system available on the internet, broke into the Administrator account using approximately 40,000 password guesses until the account was compromised. From there, the attacker was able to access CDOT's environment as the domain administrator, installing and activating the ransomware attack. The alleged attackers behind the SamSam ransomware, who operated from Iran, have been identified and are wanted by the FBI.

3. Social engineering

Social engineering is one of the most prolific and effective means of gaining access to secure systems and obtaining sensitive information yet requires minimal technical knowledge. It refers to the manipulation of individuals in order to induce them to carry out specific actions or to divulge information that can be of use to an attacker. Attacks vary from bulk phishing emails with little sophistication through to highly targeted, multi-layered attacks which use a range of social engineering techniques. Social engineering works by manipulating normal human behavioural traits and as such there are only limited technical solutions to guard against it.

Social engineering techniques are commonly used to deliver malicious software but, in some cases, only form part of an attack, as an enabler to gain additional information, commit fraud or obtain access to secure systems. Social engineering techniques range from indiscriminate wide scale attacks, which are crude and can normally be easily identified, through to sophisticated multi-layered tailored attacks which can be almost indistinguishable from genuine interactions. Social engineers are creative, and their tactics can be expected to evolve to take advantage of new technologies and situations.

Although social engineering attacks differ from each other, they have a common pattern that involves four phases: (i) collect information about the target; (ii) develop relationship with the target; (iii) exploit the available information and execute the attack; and (iv) exit with no traces (Mouton, Leenen and Venter 2016). In the research phase, also called information gathering, the attacker selects a victim based on some requirements. In the relationship phase, the attacker starts to gain the trust of the victim through direct contact or email communication. In the exploitation phase, the attacker influences the victim emotionally to provide sensitive information or perform security mistakes. In the exit phase, the attacker quits without leaving any proof (Salahdine and Kaabouch 2019).

Social engineering attacks can be classified into two categories: human-based or computer-based. In human-based attacks, the attacker executes the attack in person by interacting with the target to gather desired information. Thus, they can influence a limited number of victims. The software-based attacks are performed using devices such as computers or mobile phones to get information from the targets. In a different perspective, social engineering attacks can be classified into three categories according to how the attack is conducted: social, technical, and physical-based attacks (Kalnins, Purins and Alksnis 2017). Social-based attacks are performed through relationships with the victims to play on their psychology and emotion. These attacks are the most dangerous and successful attacks as they involve human interactions. Technical-based attacks are conducted through internet via social networks and online services websites, and they gather desired information such as passwords, credit card details, and security questions. Physical-based attacks refer to physical actions performed by the attacker to collect information about the target. An example of such attacks is searching in dumpsters for valuable documents.

4. Malware

Malware is an abbreviation of the words malicious and software. The term refers to software that is deployed with malicious intent. Malware is easy to deploy remotely and tracking the source of malware is hard. In the past decade, malware has emerged as a major threat for cybersecurity as software companies have to constantly work to write newer versions and security patches and release them so that the existing and in-use software system can be upgraded to confront new forms of threats. The financial services industry is a primary target for malware-enabled cyber-attacks because financial institutions operate software that tracks ownership of monetary assets. Cybercriminals also directly target customers of such institutions and business partners using malware-enabled attacks.

Malware may take as many forms as software. It may be deployed on desktops, servers, mobile phones, printers, and programmable electronic circuits. Sophisticated attacks have confirmed data can be stolen through well written malware residing only in system memory without leaving any footprint in the form of persistent data. Malware has been known to disable information security protection mechanisms such as desktop firewalls and anti-virus programs. Some even have the ability to subvert authentication, authorization, and audit functions. It has configured initialization files to maintain persistence even after an infected system is rebooted. Upon execution, sophisticated malware may self-replicate and/or lie dormant until summoned via its command features to extract data or erase files.

In general, a single piece of malware is generally described by four attributes of its operation - PISC (Zeltser 2010). First, propagation is the mechanism that enables malware to be distributed to multiple systems. Second, infection is the installation routine used by the malware, as well as its ability to remain installed despite disinfection attempts. Third, self-defence is the method used to conceal its presence and resist analysis, these techniques may also be called anti-reversing capabilities. Last, capabilities refer to software functionality available to the malware operator.

There are six steps a malware criminal tends to follow in order to accomplish a typical cybercrime: reconnaissance, assembly, delivery, compromise, and command (Cloppert 2010). In the beginning, the attacker surveys the target to identify points of vulnerability as well as an attack-planning phase. Then, he/she creates, customizes, or otherwise obtains malware to satisfy attack requirements. At the delivery step, the malware propagation occurs followed by the infection at the compromise level which leads to unleashing the malware capabilities at the command phase. Finally, the malware delivers data to malware operator, i.e., exfiltration, or otherwise accomplishes attack objective.

Many remarkable incidents took place in the past couple of years, and they vary in magnitude and damage level. In early 2017, the multinational credit reporting company Equifax got hacked in early 2017 and more than 800 million consumer financial data was leaked online. The hackers launched their attack by exploiting the Apache Struts vulnerability, then accessing dozens of databases and creating more than 30 backdoors into Equifax's systems. In March 2018, the US Department of Justice indicted nine Iranian hackers over an alleged spree of attacks on more than 300 universities in the United States and abroad. The hackers stole 31 terabytes of data, estimated to be worth $3 billion in intellectual property. In May 2021, the Alaska Department of Health and Social Services (DHSS) warned that a highly sophisticated cyber-attack has exposed residents' personal data, including financial information. Before systems were shut down attackers potentially had access to full names, dates of birth, Social Security numbers, addresses, phone numbers, driver's license numbers, health information, and financial information. Internal identifying numbers such as for Medicaid or case reports, and historical information concerning individuals' interaction with DHSS were also potentially exposed.

5. Deepfakes

Developments in Artificial Intelligence (AI) have led to the emergence of deepfake technologies, which pose a significant threat to American and global institutions. Deepfake is defined as an AI-based technology that can manipulate images, sounds, and video content to represent an event that did not occur (Wojewidka 2020). Deepfake technology has taken a new level of sophistication as cybercriminals now can manipulate sounds, images, and videos to defraud and misinform individuals and businesses. As a common example, there have been multiple stances where the faces of politicians are being edited onto other individuals' bodies who appear to say things that they never did.

The term deepfake is a combination of deep learning and fake. Deepfake technology is powered by a special deep learning technique, namely Generative Adversarial Networks (GANs). GANs employ two artificial neural networks working against each other in a game-like setting. A typical GAN is generally composed of two deep neural network models: a generator and a discriminator. The generator's task is to learn from the discriminator's output and thus train so that its output may deceive the discriminator. The discriminator attempts to discern if its inputs are from the genuine data set or from the adversarial data set. As described in the original work (Goodfellow et al. 2014), the competition between the two components continues until the discriminator is unable to detect media forgery, thereby improving the overall quality of the deepfake before it can be deployed.

Deepfake technology poses many threats to global public and private entities in general, and to US institutions in particular, in many ways such as defrauding businesses, conducting misinformation campaigns in politics, and raising cybersecurity concerns in enterprises. At the judicial level, evidence tampering is one of the major threats posed by deepfakes in the judicial system. Evidence in the court of law can be manipulated with the use of deepfake technology to sway a case one way or the other (Pfefferkorn 2020). At the political level, deepfakes can be quickly created and easily circulated to a wide audience to spread disinformation among the general public. Deepfake technology can be used knowingly or unknowingly to misinform the public for political advantage (Goss and Burkell 2020). At the economic level, deepfake technology has an adverse budgetary impact on businesses as it can be used to defraud them and ruin their reputations. In the same realm, face scanners that grant access to restricted areas can be breached with the use of deepfakes, which can lead to unauthorised access to sensitive information and intellectual property. Such an attack could lead to monetary loss due to the costs incurred from containing the breach, compensating customers, and heightening security costs (Rosati et al. 2017).

Several incidents took place in the past couple of years that showed the effect of deepfake technology in the political realm. One notable example was the circulation of an altered video of an American politician, Nancy Pelosi on social media. In the video, she appeared intoxicated while mispronouncing her words; the video had been viewed and shared over 2.5 million times on Facebook (Greengard 2019). On the international theater, deepfakes can have a damaging impact on geopolitics and relationships between countries. Recently, the Australian Prime Minister, Scott Morrison demanded an apology after Zhao Lijian, a spokesperson for China's foreign ministry posted a fake image on Twitter that depicted an Australian soldier holding a knife to the throat of an Afghan child (BBC 2020).

6. Insider threat

Insider threats are malicious events from people within the organization, which usually involve intentional fraud, the theft of confidential or commercially valuable information, or the sabotage of computer systems. The subtle and dynamic nature of insider threats makes detection extremely difficult. The2018 U.S. State of Cybercrime Survey indicates that 25% of the cyber-attacks are committed by insiders, and 30% of respondents indicate incidents caused by insider attacks are more costly or damaging than outsider attacks (CERT 2018).

A malicious insider is defined as "a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data, and has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems." (Costa, Albrethsen and Collins 2016). Compared to the external attacks whose footprints are difficult to hide, the attacks from insiders are hard to detect because malicious insiders already have the authorized power to access the internal information systems. In general, there are three types of insiders: (i) traitors who misuse their privileges to commit malicious activities, (ii) masqueraders who conduct illegal actions on behalf of legitimate employees of an institute, and (iii) unintentional perpetrators who innocently make mistakes. Based on the malicious activities conducted by the insiders, the insider threats can also be categorized into three types: (i) IT sabotage which directly uses IT to make harm to an institute, (ii) theft of intellectual property which steals information from the institute, and (iii) fraud which indicates unauthorized modification, addition, or deletion of data (Homoliak et al. 2019).

Insider threat research constitutes one of the facets of the new and emerging field of social cybersecurity (Carley 2020). Social cybersecurity is a computational social science with a large foot in the area of applied research. It uses computational social science techniques to identify, counter, and measure (or assess) the impact of

communication objectives. The methods and findings in this area are critical, and advance industry-accepted practices for communication, journalism, and marketing research.

Multiple noticeable insider threat incidents occurred in the last decade, whose level of sophistication ranged all over the spectrum. In Indiana in mid-2011, a foreign national with permanent residence status was convicted in the state's first ever case of insider theft. Working for two companies, he stole formulas for pesticides and food additives with the intent to establish a company in his home country with co-conspirators. The technology and the site of the theft were deliberately targeted. In Louisiana, a naturalized U.S. citizen with 27 years of service working for a U.S. chemical company conspired with former colleagues and overseas partners to steal a specific formula and market that technology to companies in his native country. In Colorado, insiders stole plans for a chip that controlled sound quality in cell phones. The insiders created a joint venture with a foreign university with the intent to mass produce the technology and market it to commercial entities.

7. Conclusion

In this paper, we provide a general overview of the main five cyber threats in the United States of America. The reader is warned that this list is by no means exhaustive, it is rather correlated with the author's expertise and fields of research. We conclude below by providing a handful of suggestions to mitigate the risks of such attacks in the near future, as well as highlight some future directions in this wide realm.

First, there are many best practices to minimize ransomware risks such as backing up data, images, and configurations in an offline pipeline, using multi-factor authentication, updating, and patching systems, making sure security solutions are up to date, reviewing the incident response plan, etc. In the United States, The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/ or fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered. Moreover, the FBI urges people to report ransomware incidents to your local field office or the FBI's Internet Crime Complaint Center (IC3). Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under US law, and prevent future attacks. As a side note, it is valuable to understand and measure the impact of a ransomware attack on the victim entity, so that adequate risk management plans can be put in place (Alhajjar and Olchowoj 2022).

Second, defense procedures for social engineering attacks include: encouraging security education and training, increasing social awareness of social engineering attacks, providing the required tools to detect and avoid these attacks, learning how to keep confidential information safe, reporting any suspected activity to the security service, organizing security orientations for new employees, and advertising attacks' risks to all employees by forwarding sensitization emails and known fraudulent emails.

Third, when planning an approach to malware prevention, organizations should be mindful of the attack vectors that are most likely to be used currently and in the near future. Malware prevention efforts such as user and IT staff awareness, vulnerability mitigation, threat mitigation, and defensive architecture are essential for the mitigation of malware attacks. An effective awareness program explains proper rules of behaviour for use of an organization's IT hosts and information. Also, a vulnerability can usually be mitigated by one or more methods, such as applying patches to update the software or reconfiguring the software.

Forth, digital forensics can provide an effective solution for detecting deepfakes. Using computational techniques, forensics experts can observe whether image pixels have been altered, by isolating anomalies, such as shadows and reflections. They can also inspect the metadata of the file to check if it has been altered, by checking the edit history and how many times the file has been compressed.

Finally, many recent works have studied ways to detect insider threats as well as find factors that lead to such incidents (Alhajjar and Bradley 2021). However, it remains a very difficult task to identify such threats, mainly because there is no straightforward way to diagnose anomalous human behavior with high certainty. A single point of anomalous behavior may not stand out, but anomalies in several areas may indicate an insider threat issue. Examples of this behavior might look like changes in job performance or work habits, downloading large volumes of information from the network, entering or exiting organization facilities at odd hours, making changes to the IT system, etc.

Acknowledgements

The second author would like to thank the Intelligent Cyber-Systems and Analytics Research Lab (ICSARL) at the Army Cyber Institute (ACI) in West Point, NY for their hospitality. Most of the work was done during his summer research stay at the institute.

References

Alhajjar, E. and Bradley, T. (2021). "Survival analysis for insider threat", *Computational and Mathematical Organization Theory*, 1-17.

Alhajjar, E. and Olchowoj, O. (2022). "The Impact of a Ransomware Attack", *Proceedings of the Sixth Annual Workshop on Naval Applications of Machine Learning, San Diego, USA.*

Alhajjar, E., Fameli, R. and Warren, S. (2021). "Are Terrorist Networks Just Glorified Criminal Cells?" *Northeast Journal of Complex Systems (NEJCS), Vol. 3: No. 1, Article 1*.

BBC (2020). "Australia demands China apologize for posting 'repugnant' fake image," [Online]. https://www.bbc.co.uk/news/world-australia-55126569. Accessed 31 October 2021.

Carley, K. M. (2020). "Social cybersecurity: an emerging science". *Computational and Mathematical Organization Theory*, pp. 365–381.

CERT (2018). "U.S. State of Cybercrime." Tech. rep. CERT Division of SRI-CMU and Force Point.

Cloppert, M. (2010). "Evolution of APT State of the ART and Intelligence-Driven Response," *US Digital Forensic and Incident Response Summit, SANS*. http://computer-forensics.sans.org.

Costa, D. L., Albrethsen, M. J. and Collins, M. L. (2016). "Insider threat indicator ontology." Tech. rep. Carnegie Mellon University, Pittsburg, PA.

Denning, D. (2000). "Cyber-terrorism". *Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services*. Washington, DC: US House of Representatives.

Farhat, V., McCarthy, B. and Raysman, R. (2011). "Cyber Attacks: Prevention and Proactive Responses", Practical Law Company.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A. and Bengio, Y. (2014). Generative Adversarial Nets. *Advances in neural information processing systems*, 2672–2680.

Gosse, C. and Burkell, J. (2020). "Politics and porn: how news media characterizes problems presented by deepfakes," *Critical Studies in Media Communication*, vol. 37, no. 5, pp. 497-511.

Greengard, S. (2019). "Will deepfakes do deep damage?" *Communications of the ACM*, vol. 63, no. 1, pp. 17-19.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y. and Ochoa, M. (2019). "Insight into insiders and IT: a survey of insider threat taxonomies, analysis, modeling, and countermeasures". *ACM Computing Surveys (CSUR)* 52.2, pp. 1–40.

Kalnins, R., Purins, J. and Alksnis, G. (2017). "Security evaluation of wireless network access points." *Appl. Comput. Syst.,* 21, 38-45.

Loman, M. (2019). "How Ransomware Attacks: what defenders should know about the most prevalent and persistent malware families," Sophos Labs white paper.

Mouton, F., Leenen, L. and Venter, H. (2016). "Social engineering attack examples, templates and scenarios." *Comput. Secur.* 59, 186–209.

Pfefferkorn, R. (2020). "Deepfakes in the courtroom," *Boston University Law Journal*, vol. 29, no. 2, pp. 245-276.

Rosati, P., Cummins, M., Deeney, P., Gogolin, F., der Werff, L., Lynn, T. (2017). "The effect of data breach announcements beyond the stock price: Empirical evidence on market activity," *International Review of Financial Analysis*, vol. 49, pp. 147-148.

Salahdine, F. and Kaabouch, N. (2019). "Social Engineering Attacks: A Survey." *Future Internet*. 11(4):89.

Wojewidka, J. (2020). "The deepfake threat to face biometrics," *Biometric Technology Today*, vol. 2020, no. 2, pp. 5-7.

Zeltser, L. (2010). "Analysing Malicious Software in Cyberforensics," *J. Bayuk, Editor, Springer*.