Section 3: Week 8: Integrating Strategic Cybersecurity

Nate Bachmeier

TIM-8301: Principals of Cybersecurity

May 23rd, 2020

North Central University

# Setting the stage

## What is Cybersecurity

CyberSecurity refers to a collection of mechanisms and processes that constrain risk to business systems by ensuring they are meet performance and consistency expectations, even under erroneous conditions (Mickens, 2018). These erroneous conditions arise due to both malicious or negligent scenarios, degrading the confidentiality, integrity, and availability of our service offerings. For instance, when two services are communicating across a private network, numerous risks to their continuity exist, such as the switch could become faulty and lossy. Security protections, like Transport Layer Security (TLS), can detect the hardware failure through checksums that are visible at the application layer. A second product defect might cause a surge of traffic, and without traffic-shaping technologies results in overloading the downstream services. A third defect might incorrectly combine data with commands, such as a single quote that triggers a SQL injection and crashing the application. From the perspective of the end-user, it does not matter if our services fail because of hardware, configuration, weak quota management, or incorrect application code. They care that the system works. These scenarios hurt the reputation of the service operators and weaken the competitive position of the business.

## How does security enable the business

Hi-Tech operates on a finite budget and must prioritize investments into features and services. On the one hand, the business would like to spend all available resources delivering its core mission, building the best electric vehicle. Allocating time and money into other projects might even appear to detract from this mission, and feel like a waste. However, investments in security aspects of the organization reduce risk and improve continuity. For instance, delivering an efficient anti-virus and patch management strategy could limit the blast radius of a malware infestation. Another example might include a collection of guard rails that prevent technicians from accidentally corrupting user data or system administrators from overwhelming the network with a misconfigured service. Hardware dies, traffic is finite, data becomes corrupt, and these incidents necessitate a methodological approach that minimizes the time to detect and recover (MTTD/MTTR).

## Framing a Security Message

Communicating the criticality of security to a broad organizational audience is challenging because too many experts have poorly framed the conversation in the past. Traditional approaches describe the Internet as being full of Boogiemen, that live in basements dressed in hoodies (de Bruijn & Janssen, 2017). These sophisticated adversaries will stop at nothing to exploit our websites and exfiltrate the data. From the employee perspective, this sounds far fetched and reminiscent of a Michael Bay film. They do not understand why they should care. Admittedly, our data is not attractive, so why would anyone bother to attack us? Instead, the message should center around the risks that our software and business processes accept-- both implicitly and explicitly. Many risks exist within technology, though a more alarming number originate from the employees (Valiente, 2017). The employees have access to customer data, production services, and other sensitive assets. When they fat-finger a database command, there is a chance of data corruption, and that will require a backup and restore operation. Fundamentally, conveying these risks results in the awareness and the formation of strategies around both prevention and recovery. Perhaps more importantly, it addresses the question, “why should I care?”

## Applying a framework to security

There is an abundance of standards and frameworks available to determine if decisions are being made consistently across the industry. Four common incarnations are the Risk Management Framework (RMF), ISO2700x, NIST Cybersecurity Framework, and COBIT v5. Each of these approaches follows a similar cycle of plan-act-assess-revise across different aspects of the stack (e.g., authentication, authorization, and auditing). However, there are differences between the degree of enforcement versus guidance. The origin of the standard also has a significant influence on the framework designers’ perspective, such as COBIT deriving from IT auditing then expanding with industry commonalities.

While each of these frameworks possesses a similar structure, they differ in terms of prescriptive guidance versus generalizations. For instance, ISO2700x has stringent requirements that necessitate a cultural shift for many businesses, and this is difficult to scale to an enterprise environment (Gillies, 2011). In contrast, the NIST Cybersecurity Framework describes various common scenarios then offers a good, better, best approach for the implementors.

Choosing a framework requires a gentle hand that is cognizant of both time and place. Introducing schedule risk to inflight commitments through abrupt policy change will always encounter political push back (Dai Zovi, 2019). For many businesses like HTM, having the flexibility to adopt a framework and then iteratively mature their processes over time reduces that risk and is an easier sell to leadership. Arguably, this is not the utopian course during the interim. However, movement in the right direction is better than no action.

# What are we protecting

## People

The most crucial resource of an organization are the employees, and any plan for success needs to begin here. Valientes (2017) estimates that nearly half of security incidents result from employee negligence, like interacting with phishing attacks and fat-fingering system commands. Businesses that focus on security awareness training can reduce these statistics and create more reliable systems. This awareness needs to touch on foreign policy expectations, like European customer data, cannot leave Europe. However, even domestic policies differ, such as California and Delaware having stricter privacy laws than federal legislation. Initially, these expectations appear arbitrary, but communications the geographical nature of the Internet presents general consistencies and best practice patterns. It also leads to an understanding of how various levels of legal enforceability influence release schedules of new features and innovation into new markets. That training can guide all levels of the organization to reach out to subject matter experts because they are aware of the inherent complexity.

It can be helpful to think of customer identity as a user profile that contains collections of historical choices, stated preferences, user roles, and known associations (Wachter, 2018). When our services understand the context of the user’s profile, the experience can be customized and produce more desirable experiences. The payment for access to these inferences and decision processes comes from personal information, such as calendars, contacts, and routines (Mickens, 2018). This trade creates privacy concerns that can be subtle and can go unnoticed for some time. For instance, numerous platforms integrate into open identity provides like Google and Facebook as a mechanism to simplify enrollment. However, is that the job the user intended to hire (Dai Zovi, 2019)? Through an exchange of convenience, the user becomes trackable across multiple sites and web services (Paller, Mahalik, Skoudis, & Ullrich, 2020). While the physical person wants a single sign-on experience, they also desire distinct virtual profiles across those providers (e.g., LinkedIn versus PornHub). Traditionally users have encountered these entanglements of context on their mobile devices, but these are not the only scenarios. Asking personal assistants, such as Siri, Alexa, and Google Home, if they spy on us, results in recommendations to review the privacy policy (Haselton, 2018). That response can be misleading since these policies exist as a liability disclaimer, not for the direct benefit of the user (Wachter, 2018).

## Processes

Protecting against foreign and domestic risks requires augmenting business processes and asset lifecycle management. Hennig (2018) recommends starting with a threat modeling to identify what resources need protection and under which contexts. During this exercise, each step needs to consider any integrity, confidentiality, and availability risks that might exist. For instance, a prerequisite of deploying web services into authoritarian nations datacenters might involve exchanging sensitive communications with a foreign company. Interception of those conversations by nation-states will occur—either across the wire or from an official subpoena. These challenges require design decisions that focus on disposable resources (e.g., one-time access tokens) and end-to-end encryption. Many real-world processes span cross-corporation and require communication across asset production, installation, operationalization, and retirement (Busdicker & Upendra, 2017). Identifying and repairing vulnerabilities across this lifecycle needs to be an iterative process that seeks feedback and incorporates it.

Manufacturing facilities are evolving into massive CPS ecosystems through Industrial IoT devices feeding into complex event processing systems (Babiceanu, 2016). This approach reduces costs by increasing automation efficiencies. Reliance on automation also increases the opacity of decision-making processes and introduces additional risk vectors (Mickens, 2018). For example, an increase in network latencies might cause decision processes to act on outdated information. When perspective distortion exists between the cyber and physical structures, then accidents can follow, like autonomous vehicles failing to stop or safety systems not initiating soon enough (Frodigh, 2018). CPS technologies can enter into this erroneous state due to Denial of Service states (DoS) caused by malicious actors, malware, and negligent administrators. Process designers need to minimize these risks by evaluating the impact of time sensitivity on their implementation.

## Products

The products released into a market need to consider the security assertions of both the foreign market and the domestic organization. For instance, authoritarian nations will steal innovations and share those trade secrets with foreign competitors. The inverse can also be true, where products lack the security assertions of the foreign market and are not permissible. Recently Kaspersky Anti-Virus was banned from several American institutions because of concerns that Russia could maliciously control the software (Krebs, 2019). This trait is not unique to authoritarian nations, as specific New Zealand products have been ban from France for not meeting privacy norms (Hunt, 2019). When a product does not meet the expectations of either the producer or the consumer, then a decision around acceptable risk needs to take place. Those decisions might result in bundling fewer features into a smaller version or blocking the deal entirely.

There is an economic incentive for businesses to churn out new products and devices with more innovative, instead of investing in security protections for those features (Li & Liao, 2018). For many retail markets, the customer makes purchasing decisions predominantly on which product has the most features at the lowest price. Meanwhile, devices such as 8-bit micro-controllers, lack the computing resources necessary to support authentication, authorization, auditing, and transport encryption (Weber & Studer, 2016). Even when there are sufficient resources available, security protections can cause interoperation (interop) challenges, which leads to customers assuming that the product does not work. If the customer believes that the offering is faulty, they leave bad reviews online, contact support, and request replacements—all of which cost the business money.

# Whom are we defending against

## Negligence

When we step back and look at the numbers, half security incidents come from employee negligence. Their interaction with hostile automation, e.g., phishing attacks and malicious mobile apps, along with trying to find the path of least resistance for completing their job—bypasses safety protocols. Malicious actors (e.g., scam artists) and technical glitches account for the remainder. Those figures suggest that creating a more security-aware culture could remove nearly half of the attack surface and strengthen business continuity (Valiente, 2017). For instance, when network engineers understand risk management, they create features that consider scalability and availability during the design versus after the solution has failed(Mickens, 2015). It is too late to discuss service redundancies and fail-over technologies after the service is offline, or least privileges after a support technician accidentally corrupts customer data. These challenges will continue to occur until there is sufficient awareness, and team members understand the damage that follows their actions. If we can at least stop the good guys doing bad stuff, the organization would be in a much better position.

## International actors

### Cyberespionage

Businesses that operate solely within the United States have access to a legal system that enables seeking damages for malicious third-party behavior. For instance, when Uber stole intellectual property from Google, it was sued for $250M in damages (Bensinger, 2019). When the same theft occurs across international borders, jurisdiction becomes less clear and is more challenging to enforce. Participants in these hostile markets need to be aware that espionage comes from various sources, such as individual hackers and nation-states (Krebs, 2019). International law does not prohibit these nation-states spying, Article 51 of the United Nations charter even allows it under the disguise of self-defense (Banks, 2017). Some states argue that different rules should exist for monitoring public and private institutions. However, this perspective employs a very Western view. For socialist countries, the distinction is fuzzier than a purely capitalist society as the boundary between the industries lacks a consistent definition.

### Cyber sabotage

Using technologies like ransomware, malicious software that encrypts digital devices, nefarious actors can force an organization to purchase decryption keys before restoring service (Busdicker & Upendra, 2017). Attackers also send high volumes of network traffic into corporate websites as a mechanism causing Denial of Service (DoS) scenarios. When these cyber sabotage events occur, it disrupts business continuity and impacts the credibility of the victim. American companies have traditionally relied on deterrence, such as the Computer Fraud and Abuse Act (Fischerkeller & Harknett, 2017). Technological solutions like deploying applications across multiple Public Cloud Service Provider (CSP) data centers can minimize the influence of DoS attacks. However, these same legal protections do not uniformly exist across the globe, and regulations around data placement can limit the accessibility of flexible fail-over solutions.

### Subversion

The international community does not agree on the strict definition of what constitutes a cyber-attack (Fischerkeller & Harknett, 2017). These differences influence auditing and compliance requirements between countries and prevent direct comparisons across policies or statistics (Matsubara, 2014). The political values of nations contribute to the disparity, such as Europe prioritizing end-user safety versus authoritarian governments preferring to save face. When requirements around transparency do not fully exist, then even legitimate partners are unlikely to tell the whole truth. Being the only business that is forthcoming creates a competitive disadvantage, as customers only see “A” claims to be more secure than “B.” Without a carrot or stick, how can a domestic company ensure security incidents are timely and accurately communicated? Imagine the challenges with less reputable entities, if these are the risks with legitimate partners.

## Scammers, Spammers, and Robots

Attacks from these anonymous guests is another evolving area. Where former hackers would carry out manual attacks, those with botnets could use automation to increase their leverage. However, in the modern world, the ubiquitous availability of cloud and high-speed networking removes these artificial constraints. Now, anyone with a few dollars and an open-source vulnerability scanner can programmatically cluster targets and attack the signature as a whole (Dai Zovi, 2019). Substantial effort goes into protecting these platforms, but little attention considers the other side of the equation—all of these people (Blythe & Coventry, 2018). Modern enterprise networks have hundreds of users that are authorized to perform tasks. When those users fail, it can be very challenging to detect, mitigate, or even control the blast radius (Elifoglu, Abel, & Tasseven, 2018). This realization creates the need for security engineers to design programs that center around awareness and skepticism.

# How are they attacking us

## Ransomware and Malware

Malicious software, or malware, are applications that compromise the confidentiality, integrity, or availability of a system. These programs infect systems via email, file-sharing services, browser vulnerabilities, spoofed resources, and misconfigured services (Lee, Moon, & Park, 2017). It can be challenging to contain the spread through an organization due to homogeneous configurations of the devices. For instance, a branch office will likely run the same software packages on each workstation and share documents through central repositories. The objective of the malware can vary from scenarios such as remote command-and-control, data exfiltration, and denial of service scenarios. One specific attack that is gaining popularity is ransomware, which are applications that encrypt user data and then offer to sell the decryption key (Busdicker & Upendra, 2017). Since malware comes from different vectors with varying objectives, detecting and preventing all scenarios is nearly impossible. Even with protection against all known scenarios, criminal social networks have easy access to exploitation packages and zero-day vulnerabilities across the dark web (Ericsson, Almukaynizi, Nunes, & Shakarian, 2018). Given the availability of exploitation software, organizations need to consider these scenarios as part of their risk management planning. Addressing these unknown unknowns requires defense-in-depth mindsets that expand beyond edge firewalls to include more robust Intrusion Detection and Prevention Systems (IDS/IPS).

## Patch Management and Zero Days

Zero-day black markets allow governments, criminals, and researchers to transact in weaponized exploits (Emery, 2017). Defenses against these attacks do not exist, enabling the holder to access the vulnerable system instantly. However, the more common scenario is that an attacker will use a known vulnerability that is over a year old (Galinec & Steingartner, 2017). Not only does patch management address the default scenario, but also it is a cheaper problem to solve. Addressing patch management requires two components; first notification to employees that updates are available and second training to apply them. Through security training, the staff can be made aware of why the updates are necessary and the reasons for the timely application. While it can be challenging to mandate software patching, especially in Bring Your Own Device (BYOD) scenarios, network administrators can integrate compliance checks into connectivity lifecycles (e.g., during VPN authorization).

## Phishing

Users interact with spoofed resources through cold-calling or name squatting scenarios, such as emails directing them to netflix.com.evil.com. Previous security messages tell the user to look for details, like misspellings, as evidence of being fake (Proctor & J, 2015). However, this implicitly implies that perfect grammar infers being real. When users connect to websites, training has also told them to look for the security icon, but this only means the traffic is encrypted (Hunt, 2019). Without a consistent and reliable method to determine that a resource is genuine, the only alternative is skepticism. For instance, when a banker calls for account information, hang up and call them back through the main switchboard. If the call were real, there would be a note on the file, and another representative will assist. Along those same lines, if netflix.com.evil.com, needs an update to your information, start at Bing and search for Netflix login, scrolling past the advertisements to the real site. While none of these methods are fool-proof, they increase the odds of ending at the right location.

# Examine Evolution of Attack Surface

## Abstract Borders, Cloud, and XaaS

Traditional cybersecurity solutions focus on hardening the network parameter with firewalls and vulnerability scanners. However, this approach is no longer sufficient as attackers center their efforts on the application layer (Astani & Ready, 2016). By design, anonymous users can interact with the organization through public interfaces, such as web services and email. When malicious actors exploit Structured Query Language Injections (SQLi) or embed ransomware into mail attachments—it bypasses these network barriers and allows unauthorized access to information. Further complicating matters, the boundary of the network is becoming more abstract due to the notion of “everything as a service” (Paller, Mahalik, Skoudis, & Ullrich, 2020). For instance, 40% of enterprises are in the process of uplifting mission-critical services, like identity and authorization, into third-party providers (Galinec & Steingartner, 2017). Shifting ownership to these provides does not mean transferring the responsibility of risk. Users do not care if DropBox or Amazon owns the physical server—they entrusted the stewardship of their data to HTM and will blame them for negligent handling. Modern businesses need to evolve their controls to meet the challenges of these application-specific vulnerabilities using strategies that encompasses people, processes, and products.

## Geography and Sovereignty

The premise of the Internet is an open communication system that connects people from around the world, enabling commerce and ideas to flow freely. However, nation-states also want to protect their sovereignty and enforce laws around these interactions (Inkster, 2015). These competing requirements cause national security policies to make trade-offs between government control, societal freedoms, and rights of international actors (Kovacs, National cybersecurity as the cornerstone of national security, 2018). Since the values of democratic and authoritarian nations vary substantially, it is unrealistic to assume a unified set of policies can exist that appeal to all countries. Instead, nearly all nations legislate laws that target the Internet infrastructure that resides within their state (Matsubara, 2014). These decisions create geography that influences the protective capabilities and behavioral norms. For instance, the European Union (EU) believes that building a digital economy begins with user privacy(Kovacs, 2017). While the EU’s Global Data Protection Regulations (GDPR) mandates severe penalties for negligence, like data breaches, authoritarian countries such as Russia are more laisse-fair. These value differences appear in other aspects like the transparency to share evidence or assist with criminal investigations.

## IoT

The Internet of Things (IoT) represents the next evolutionary step in communication and system connectivity. Naïve outsiders see this industry as a series of gimmicks, Apple watches, and smart toasters. Those statements are right, but more importantly, it also creates the missing bridge between cyber and physical systems (CPS). This capability comes from sensor and input networks that emit telemetry into ubiquitous cloud computing and machine learning platforms. Using physical motors and actuators, artificial intelligence and big data solutions can then reach back into manufacturing and safety systems. As information and decision processes transact across this bridge, it enables organizations to execute expert workflows autonomously and prevent costly failures. However, many challenges exist around ensuring the confidentiality, integrity, and availability (CIA) of all participants of this system.

According to Gartner, the trend of weak authentication controls impacts nearly 50% of all IoT vendors (Galinec & Steingartner, 2017). The Mirai malware was able to span half a million devices using a small dictionary file to brute force access (Gamblin, 2017). Although its source code has been available for several years, and its particularly noisy approach to gaining entry are discoverable, variations are still thriving (Kolias, Kambourakis, Stavrou, & Voas, 2017). While these programs should have encouraged a movement toward security by default, the broad industry has failed to act against even this rudimentary attack.

# Prioritizing Risk Management

Finite resources Translating the protection requirements into security implementations have a wide range of maturity levels that could follow a good, better, best approach. Ideally, Hi-Tech would only follow the most strict guidelines. However, that is not as practical due to unacceptable costs both financially and in terms of user experience. For example, the business uses many IoT devices that lack remote firmware upgrade capabilities. It might be acceptable to have the operations team manually upgrade each device annually—though the labor costs are too high for monthly cadences. In many scenarios, choosing a security investment is not binary (do everything versus do nothing). Instead, the purchase can be in the middle and follow a phased release (Gordon, Loeb, Lucyshyn, & Zhou, 2015). This approach could divide the upgrade task into subgroups based on the criticality, like safety systems versus temperature sensors. Each subgroup can feed into the prioritization discussion, perhaps resulting in safety systems landing on a quarterly upgrade cycle, and the less critical sensors remain on an annual cycle. This decomposition of large bodies of work keeps the costs down and enables more focused efforts.

Vulnerabilities exist at the intersect of three conditions. “(1) system susceptibility, such as a design or implementation flaw; (2) threat accessibility, such as system access points or services; (3) threat capability, such as an opponent with the knowledge and resources to discover, access, and exploit a flaw” (Baskerville, Rowe, & Wolff, 2018, p. 35). Often, it can be more economical to address one of the other criteria than the underlying problem. For instance, the IoT temperature sensors have a well-known remote command execution defect in the File Transfer Protocol (FTP) daemon. If Hi-Tech does not rely on this functionality, then merely blocking access at the network switch level removes the issue. Another vulnerability exists in the Telnet daemon communicating in plain-text. Similarly, the administrators can place those interactions on a Virtual Local Area Network (VLAN) to limit access.

There can be political pushback that some protections come with a cure worse than the disease. Hi-Tech would desire that leadership signs off on every work order, which is not feasible given the competing demands for time. Some staff members are aware of an override code to bypass this requirement and get the invoices out the door. While the rule intends to ensure that invoices are complete and promote accountability, it also causes a bottleneck that impedes timely delivery. On the one hand, the security team could remove the bypass feature, but this introduces additional work for the team. Approaching the prioritization of these scenarios requires a gentle touch, as security enables the business, not the other way around (Dai Zovi, 2019). Instead, a conversation could begin with senior leadership to understand if the previous decision still makes sense. If the idea is valid, perhaps minor tweaks can maintain the central concept under more amenable terms.

Another challenge comes from balancing security over the rapid development of new features (Lam, 2016). Hi-Tech follows a three-month Water Flow Release Cycle that plans, implements, stabilizes for three, six, and three weeks respectively. Once the planning is complete, it can be challenging to introduce additional work as it requires an expensive reset. If the security team is divorced from this cadence, there is a high risk to existing business commitments. While the senior leadership team might be willing to accept those scheduling challenges, it puts unnecessary stress on the teams. For instance, postponing the release might delay a big customer onboarding into the platform. Ultimately these decisions are trading one set of risks for another.

# References

Astani, M., & Ready, K. (2016). Trends and preventive strategies for mitigating cybersecurity breaches in organizations. *Issues in Information Systems, 17*(2), 208-214. Retrieved May 9th, 2020, from https://iacis.org/iis/2016/2\_iis\_2016\_208-214.pdf

Babiceanu, R. &. (2016, September). Big data and virtualization for manufacturing cyber-physical systems. *Computers in Industry, 81*, 128-137. doi:https://doi.org/10.1016/j.compind.2016.02.004

Banks, W. (2017). Cyber espionage and electronic surveillance: beyond the media coverage. *Emory Law Journal, 66*(3), 513-525. Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=ofs&AN=121933698&site=eds-live

Baskerville, R., Rowe, F., & Wolff, F. (2018, February). Integration of information systems and cybersecurity countermeasures. *Special Interest Group on Management Information Systems (SIGMIS) Databases, 49*(1), 33-52. doi:https://doi.org/10.1145/3184444.3184448

Bensinger, G. (2019). *Former Google self-driving engineer, who prompted a lawsuit against Uber, gets hit with criminal charges*. Retrieved from Washington Post: https://www.washingtonpost.com/technology/2019/08/27/former-google-self-driving-engineer-who-prompted-lawsuit-against-uber-gets-hit-with-criminal-charges/

Blythe, J., & Coventry, L. (2018, October). Costly but effective: comparing the factors that influence employee anti-malware behaviors. *Computers in Human Behavior, 87*, 87-97. doi:https://doi.org/10.1016/j.chb.2018.05.023

Busdicker, M., & Upendra, P. (2017). The Role of Healthcare Technology Management in Facilitating Medical Device Cybersecurity. *Biomedical Instrumentation & Technology Sep; Vol. 51 (s6)*, 19-25.

Dai Zovi, D. (2019). Every Security Team is a Software Team Now. *Blackhat USA.* Black Hat. Retrieved May 2020, from https://www.youtube.com/watch?v=8armE3Wz0jk

de Bruijn, H., & Janssen, M. (2017, January). Building cybersecurity awareness: the need for evidence-based framing strategies. *Government Information Quarterly, 34*(1), 1-7. doi:https://doi.org/10.1016/j.giq.2017.02.007

Elifoglu, H., Abel, I., & Tasseven, O. (2018). Minimizing insider threat risk with behavioral monitoring. *Review of Business, 38*(2), 61-73. Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=bth&AN=129631258&site=eds-live

Emery, A. (2017, Summer). Zero-day responsibility: the benefits of a safe harbor for cybersecurity research. *Jurimetrics: The Journal of Law, Science & Technology, 57*(4), 483-503. Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=a9h&AN=126542986&site=eds-live

Ericsson, M., Almukaynizi, M., Nunes, E., & Shakarian, P. (2018). Community finding of malware and exploit vendors on dark web marketplaces. *1st International Conference on Data Intelligence and Security*, 81-84. South Padre Island, TX, USA. doi:https://doi.org/10.1109/ICDIS.2018.00019.

Fischerkeller, M., & Harknett, R. (2017). Deterrence is not a credible strategy for cyberspace. *Orbis, 61*(3), 381-393. doi:https://doi.org/10.1016/j.orbis.2017.05.003

Frodigh, M. (2018, May 27th). Keynote Opening. *40th International Conference on Software Engineering.* Gothenburg, Sweden: International Conference on Software Engineering (ICSE). Retrieved April 8th, 2019, from YouTube: https://www.youtube.com/watch?v=cpeMmMh7Syk

Galinec, D., & Steingartner, W. (2017). Combining cybersecurity and cyber defense to achieve cyber resilience. *14th International Scientific Conference on Informatics.* Poprad, Slovakia: Institute of Electrical and Electronics Engineers. doi:https://doi.org/10.1109/INFORMATICS.2017.8327227

Gamblin, J. (2017, July 15th). *Mirai-Source-Code*. Retrieved May 17th, 2020, from GitHub: https://github.com/jgamblin/Mirai-Source-Code

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *TQM Journal, 23*(4), 367-376. doi:http://dx.doi.org.proxy1.ncu.edu/10.1108/17542731111139455

Gordon, L., Loeb, M., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment. *Journal of Accounting and Public Policy, 34*(5), 509-519. doi:https://doi.org/10.1016/j.jaccpubpol.2015.05.001

Haselton, T. (2018). *I asked Siri, Alexa, and Google Assistant if they are spying on me — here is what they said*. Retrieved May 17th, 2020, from CNBC: https://www.cnbc.com/2018/05/13/are-siri-alexa-and-google-assistant-spying-on-me.html

Hunt, T. (2019, May 20th). *Keynote: Hack to the Future*. Retrieved from YouTube: https://www.youtube.com/watch?v=qCOefMiakps

Inkster, N. (2015). Cyber espionage. China’s Cyber Power. *Adelphi Series, 55*, 51-82. doi:https://doi.org/10.1080/19445571.2015.1181439

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer, 50*(7), 80-84. doi:https://doi.org/10.1109/MC.2017.201

Kovacs, L. (2017). Cybersecurity policy and strategy in the European Union and NATO. *Revista Academiei Fortelor Terrestre, 23*(1), 16-24. Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=a9h&AN=128789540&site=eds-live

Kovacs, L. (2018). National cybersecurity as the cornerstone of national security. *Revista Academiei Fortelor Terrestre, 23*(2), 113-120. Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=a9h&AN=130455890&site=eds-live

Krebs, C. (2019, April 23rd). ICCE 2019 - Keynote by Christopher Krebs, Director, Cybersecurity, and Infrastructure Security Agency. Retrieved from YouTube: https://www.youtube.com/watch?v=aVfcgNhHSDM

Lam, W. (2016). Attack-prevention and damage-control investments in cybersecurity. *Information Economics and Policy, 37*, 42-51. doi:https://doi.org/10.1016/j.infoecopol.2016.10.003

Lee, J., Moon, S., & Park, J. (2017, July). CloudRPS: a cloud analysis based enhanced ransomware prevention system. *Journal of Supercomputing, 73*(7), 3065-3084. doi:https://doi-org.proxy1.ncu.edu/10.1007/s11227-016-1825-5

Li, Z., & Liao, Q. (2018, January). Economic solutions to improve the cybersecurity of governments and smart cities via vulnerability markets. *Government Information Quarterly, 35*(1), 151-160. doi:https://doi.org/10.1016/j.giq.2017.10.006

Matsubara, M. (2014). Countering Cyber-Espionage and Sabotage. *RUSI Journal: Royal United Services Institute for Defence Studies, 159*(1), 86-93. doi:https://doi-org.proxy1.ncu.edu/10.1080/03071847.2014.895263

Mickens. (2018, August 16th). *Why Do Keynote Speakers Keep Suggesting That Improving Security Is Possible?* Retrieved from YouTube: https://www.youtube.com/watch?v=ajGX7odA87k

Mickens, J. (2015, September 9th). *Not Even Close, The State of Computer Security with Slides*. Retrieved May 24th, 2020, from YouTube: https://youtu.be/tF24WHumvIc

Paller, A., Mahalik, H., Skoudis, E., & Ullrich, J. (2020). The five most dangerous new attack techniques and how to counter them. *RSA Conference.* RSA. Retrieved May 9th, 2020, from https://youtu.be/xz7IFVJf3Lk

Valiente, C. (2017, October). Addressing Malware WITH Cybersecurity Awareness. *Information Systems Security Association Journal, 15*(10), 16-22. Retrieved from https://search-ebscohost-com.proxy1.ncu.edu/login.aspx?direct=true&db=tsh&AN=125478200&site=eds-live

Wachter, S. (2018, June). Normative challenges of identification in the Internet of Things: privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review, 34*(3), 436-449. doi:https://doi.org/10.1016/j.clsr.2018.02.002

Weber, R. H., & Studer, E. (2016, October). Cybersecurity in the Internet of Things: Legal aspects. *Computer Law & Security Review, 32*(5), 715-728. doi:https://doi.org/10.1016/j.clsr.2016.07.002