USF | Muma Case Review
A publication of the Muma College of Business | University of South Florida

Volume 3 Number 8 09 MAY 2018

ED FULFORD

A NOTE ON THE CYBERSECURITY PROBLEM SPACE IN 2018[1]

The Transmission Control Protocol/Internet Protocol (TCP/IP) used for Internet communications was designed so that traffic from one device connected to the Internet was visible to all other connected devices. This one attribute made it possible for bad actors and hackers to attack any company, country, or person from anywhere on earth across the Internet. For the first time in recorded history, a disgruntled individual, terrorist group, or rogue country wreaked havoc on other people, companies, countries, and--of even greater concern--the global economy. All that was required was a computer, an Internet connection, and one or more vulnerable endpoints attached to critical applications or networks also linked to the Internet.

The cybersecurity industry had long acknowledged that the Internet was not originally designed for electronic business. Also, it was never intended for the transmission of critical information, nor for the support of mission critical networks and infrastructure. As quoted from a 2002 research report produced by the CERT Coordination Center in connection with the Software Engineering Institute (SEI) at Carnegie Mellon University (CMU): “The Internet was not designed to resist highly untrustworthy users” (Lipson, 2002).

Recognizing this problem, the cybersecurity industry’s mindset was focused on defending against untrustworthy users. After all, this approach worked in the physical world. If one knew the weapon that an attacker was using and the direction from which the attack was coming, an effective defense could often be planned and implemented. However, this had not been the case when defending against cyberattacks on the Internet. There usually were many ways to stage an attack without being detected. In addition, the technologies that were used for masking such attacks had become more sophisticated, as demonstrated by attackers’ abilities to anonymize themselves and their attack vectors, which made it much more difficult to isolate the sources of attacks. Also, remember that many of the recent cybersecurity solutions defended against an attack that had already occurred and offered no assurance that they could defend against the next attack.

Cybersecurity and risk management professionals had been working diligently to improve information security and risk management practices in order to reduce overall cybersecurity risks. While these efforts had managed to improve information security practices, they had done so without showing any significant or maintainable reductions in the numbers and types of cybersecurity risks. This situation had identified a variety of challenges that cybersecurity experts needed to address in a number of key problem areas.

[1] Copyright © 2018, *Ed Fulford*. This technical note was developed to provide background information in support of one or more case studies published by the *Muma Case Review*. It may be freely copied and shared for non-commercial purposes.

Editor: T. Grandon Gill, DBA

The Cybersecurity Problem Space

Ely Kahn from Sqrrl, one of responders to the 2017 Passcode (The Christian Science Monitor's section on security and privacy) poll of cybersecurity practitioners, stated (Sorcher, 2017):

> *I think the most urgent cybersecurity challenge is the need for all organizations to fully understand the cyber risks they face, how those risks affect their mission, and what are the most cost-effective ways to mitigate those risks.*

The cybersecurity practitioners' struggles to stem the tide of cyber risks came at the increasing expense of the resources--tools, personnel, and support--needed to change the nature of global, national, and business behaviors that helped create this situation in the first place. The focus on creating cybersecurity solutions to fix more than point problems had not gained significant mindshare with cybersecurity practitioners, so they tried to transform current information security and risk management approaches to address broader and increasing more interrelated problem spaces. As a method of dealing with cybersecurity risks, information security might ultimately have had an indirect impact on the successful implementation of effective cybersecurity control programs over time. However, the management and assessment practices related to information security problem and solution spaces were not encompassing enough and were too inwardly focused to enable wide-reaching strategic and tactical enhancements to take place. As such, cybersecurity programs were not maturing quickly enough to deal with these risks. One significant reason for this situation was the lack of collaboration between companies that did business together. In many cases, these business partners did not discuss their common cybersecurity issues because of the lack of defined rules of engagement and secure communication capabilities.

For the purpose of this article, the following cybersecurity problem areas will be discussed:

- Global Cybersecurity Problems
- Government Cybersecurity Problems
- Business Cybersecurity Problems
- Cybersecurity Standards Problems

Global Cybersecurity Problems

Europol, the European Union Agency for Law Enforcement Cooperation, recently assessed the global impact of cybersecurity events like the ransomware epidemic. In their study, they found that their efforts had some successes in disrupting criminal groups that primarily operated online. However, they also determined that the economic impact was far reaching with cross-border implications as multinational banks and international corporations were attacked. Commenting on this situation in an October 2017 interview published on HelpNetSecurity.com, Europol's Executive Director Rob Wainwright stated ("The Global Impact," 2017):

> *The global impact of huge cyber security events such as the WannaCry ransomware epidemic (a cryptoworm attack in 2017 which targeted computers running the Microsoft Windows operating system by encrypting data and then demanding the owners to make payments in the Bitcoin cryptocurrency to release the computer has taken the threat from cybercrime to another level.*

Summing up the efforts of Europol and its law enforcement partners at the conclusion of the interview, Wainwright said that, even with the progress that had been made, "The collective response is still not good enough" ("The Global Impact," 2017).

Over time, cybersecurity threats and attacks like the WannaCry incidents had become ever-present news items. As terrorist groups and rogue governments sought new ways to economically damage or strike fear in their enemies, the number and sophistication of cybersecurity incidents grew. The 2017 Internet Organised Crime Threat Assessment cited several examples of cyber events with a global reach that included:

- Ransomware eclipsed most other cyber-threats with global campaigns indiscriminately affecting victims across multiple industries in both the public and private sectors. Some attacks targeted and affected critical national infrastructures at levels that could have endangered lives. These attacks highlighted how network interconnectivity, poor digital hygiene standards and insufficient security practices allowed such threats to quickly spread and expand the attack vectors.

- The first serious attacks by botnets using infected insecure Internet of Things (IoT) devices occurred.

- Data breaches continued to result in the disclosure of vast amounts of data, with over 2 billion records related to European Union citizens reportedly being leaked over a 12-month period, often exacerbated by poor digital hygiene and security practices.

- The Darknet remained a key cross-cutting enabler for a variety of crime areas. It provided access to among other things:

    - The supply of drugs such as Fentanyl and new psychoactive substances which directly led to many fatalities internationally

    - The supply of firearms that were used in terrorist acts

    - Compromised payment data which enabled bad actors to commit various types of payment fraud

    - Fraudulent documents which facilitated various types of fraud, trafficking in human beings, and illegal immigration activities

- Offenders continued to abuse the Darknet and other online platforms, sharing and distributing child sexual abuse material, and engaging with potential victims, often coercing or sexually extorting vulnerable minors.

- Payment fraud affected almost all industries, having the greatest impact on the Retail, Airline and Accommodation sectors. Several sectors had been targeted by these fraudsters as the services they provided could be used for the facilitation of other crimes, including trafficking in human beings or drugs, and illegal immigration.

- Direct attacks on bank networks manipulated card balances, took control of ATMs or directly transferred funds, known as payment process compromise, represented one of the serious emerging threats in this area. (“The Global Impact,” 2017).

While governments began to allocate more money and personnel to defend their countries, many companies were not financially able to defend themselves, and affected individuals were even less able to do so. Even with the regulatory and industry requirements placed on them, neither companies nor individuals could adequately defend themselves from cyber-attacks and were not likely to have the training, competence, or capability to do so. The best that could be expected was that companies would continue to strive to maintain a heightened degree of operational resilience, business continuity, and disaster recovery in their strategic and tactical plans.

As outlined in the cybersecurity industry report mentioned above, international and business boundaries had been all but eliminated by electronic commerce, which put more pressure on governments and companies to be more vigilant in their own cybersecurity controls to prevent or limit the impacts from cyber incidents. Practitioners in the cybersecurity field actively discussed if it was more prudent to implement, maintain, and monitor the effectiveness of security controls around their supply chains or their networks. Ultimately, however, these cybersecurity professionals determined that more work was required. In many cases, the international supply chains were intertwined with transnational computer networks, which made the deployment and monitoring of these security control mechanisms and systems much more difficult. As discussed previously, the lack of cybersecurity program maturity in governments and international companies, in addition to the absence of consistent collaboration between these groups based on prescribed rules for doing so, limited their abilities to coordinate actions to deal with cybersecurity issues that arose on a seemingly daily basis.

The consequences from the set of circumstances outlined above were far-reaching. For example, the rising hostility of threat actors was often misunderstood and not foreseen before attacks took place, which lessened the time and ability for governments or companies to respond, thus costing them financially and operationally as well as negatively impacting their reputations. The other effects from such events included critical systems and services not being available or functioning as designed during emergencies and the civil conflicts that resulted from prolonged service outages.

Government Cybersecurity Problems

Government agencies had helped safeguard very sensitive information on their country’s citizens as well as data about their actions and programs that affected the public welfare. This had made them particularly attractive targets for cyberattacks. Unfortunately, governments had often lagged behind businesses in the implementation of cybersecurity controls and protection systems. This became a serious concern as the cyberattacks and the terrorists who launched them became more sophisticated. The Heritage Foundation, in its January, 2018 report on Federal cyber breaches, found that there were over 30,000 cybersecurity incidents that affected the United States government in 2016, with 16 rising to the level of a being a major incident (Walters, 2018). Both the Obama and Trump Administrations issued Executive Orders mandating the United States government to implement modern, focused, responsive, and proactive cybersecurity programs that had the ability to adapt to the threat environment and to provide better measurements of the cyber risks faced. At this point, it was not readily apparent that the government had begun to dedicate the appropriate resources to do this and to meet these cyber challenges in an aggressive way.

Cybersecurity practitioners both inside and outside the government questioned what intelligence and law enforcement agencies had done to deploy effective cyber defense technologies. Of particular concern were the abilities of agencies charged with cybersecurity monitoring as well as identifying and remediating security breaches. For example, when Wikileaks released what it believed to be a list of CIA hacking tools in March, 2017, these abilities were seriously questioned. This incident exposed a list of cybersecurity hacking applications known as “Year Zero” or “Vault 7,” which were reportedly acquired by Wikileaks while the information passed between government employees and contractors in an “unauthorized manner.” A month later in April, 2017, a group known as the Shadow Brokers continued releasing what it claimed were NSA hacking tools. One of the tools included in this release, known as

EternalBlue, was associated with a number of cyberattacks, including those involving WannaCry ransomware, which occurred throughout the summer of 2016 and into 2017. The Shadow Brokers claimed to have stolen these tools from a team, known as the “Equation Group,” which was reportedly associated with the NSA (Walters, 2018).

Also, state and local governments had been even more at risk from such cyberattacks. Few had the money to invest in the technologies and the appropriately trained personnel to provide needed services in network security, threat intelligence, risk-based analytics, and data encryption. The ransomware attack that crippled the government support systems of the City of Atlanta, Georgia for over a week in March, 2018 was further indication that local governments had been woefully underprepared from a technical capability perspective and a personnel standpoint to deal with these types of cyberattacks when they occurred (Hutcherson, 2018).

Government agencies at all levels had not been able to effectively create cyber defense capabilities in their organizations, primarily due to the fact that their cybersecurity strategies had often been “siloed” in one functional area. As such, these agencies had not concentrated on bringing their entire organization up to a baseline level of compliance to cybersecurity standards such as those created by the National Institute of Standards and Technology (NIST). By assessing their current cybersecurity strategies and competencies against these standards, agencies determined what gaps existed in their processes and practices as well as in their technical capabilities. This began to help them determine how exposed their information assets were and the best ways to resolve those security control issues.

From a functional standpoint, government agencies needed to build more robust security-focused cultures that monitor, measure, and manage cybersecurity behaviors. Once this had been initiated, agencies then concentrated on pushing out cyber risk management activities to the rest of their organizations. Providing the right visibility to, and understanding of, cyber risks to the broader organization was found to be critical to success in mitigating them quickly and minimizing their impacts.

Collaboration and communication of potential and real cybersecurity events and attack scenarios showed that such activities facilitated agencies working better together. This information sharing assisted agencies in better understanding cyber incidents that had the potential to affect agencies and other public organizations. By identifying critical points of failures, decision criteria, and barriers to progress, government agencies had developed better cyber defense strategies that speeded remediation from breaches and prevented similar events from occurring in the future. In the Heritage Foundation’s report, one of the key takeaways was that the United States government should continue to focus on securing its own networks while collaborating with the private sector and international communities on better understanding cyber risks. (Walters, 2018).

In order to change the behaviors in government agencies, the numbers and types of cybersecurity threats and vulnerabilities had been evaluated in more detail, including the activities of foreign and domestic cyber threat actors and their attendant risks. This had shown the potential to speed up the implementation of cyber risk management technologies to defend against these actors. This had also assisted with better aligning cybersecurity strategies with those of the agencies’ operational missions. Government agencies had not consistently created and tested cyber defense readiness plans. When done proactively, these programs had success in ensuring that incident response and escalation procedures were widely communicated and tested for their effectiveness. Additionally, this facilitated collaboration between agencies to show how they jointly managed cyber incidents. In the law enforcement arena, programs like the Department of Justice’s Building Communities of Trust initiative improved how federal and local law enforcement groups worked together. (Wasserman, 2010).

Finally, government agencies had not had the appropriate levels of internal expertise required to make better cybersecurity investment and program management decisions. Agencies needed to examine their cybersecurity investments against leading practices and benchmarks, but this had not been done consistently. In order to ensure agencies allocated their resources with a risk-based approach, they had utilized mission objectives, benchmarks, and cybersecurity directions as guides. Government agencies had approached their cybersecurity postures as an evolving landscape of increasing potential threats--one that had required the ability to adapt to those risks. Proactive and mature cybersecurity programs had needed the commitment from leaders to be able to invest wisely, create a culture of cyber innovation, and maintain relevant and continuous training and awareness programs.

Business Cybersecurity Problems

Cybersecurity had become one of the most important issues facing businesses today. According to the World Economic Forum’s 2018 Global Risks Report, both large-scale cyberattacks and major data breaches or fraud were ranked among the top five most likely risks in the next decade (“The Global Risks Report,” 2018). At the time of the case, companies had been required to deal with cybersecurity problems head on because those issues have had significant impacts on the overall business operations as well as the Information Technology (IT) infrastructure. This had become even more critical for those businesses that were interconnected with third parties such as partners and suppliers. These interconnections exposed all the business partners to cyber threats that had become more severe and frequent. As the numbers of security risks had risen, businesses learned, to their dismay, that they faced more threats and more attacks than ever before, many of which required more and faster cyber response and remediation capabilities than were already in place.

As businesses expanded their interconnections and shared more information, the number of networks and devices that required more comprehensive security controls increased as well. In recent years, 63 percent of breaches were traced to third-party vendors, according to the Soha System’s 2016 survey on third-party risk management (“Soha Systems' Survey,” 2016). The security of mobile telephones, tablet computers, and other networkable devices had lagged in the implementation of cybersecurity controls too. Additionally, new technology advances such as artificial intelligence and machine learning enabled threat actors to create more malicious and sophisticated tools to use in their attacks.

If the statistics from recent global security breaches had been accurate indicators, the impacts of these incidents clearly affected businesses and their partners as a group as well as individually. In a November, 2017 article on ComputerWeekly.com, incidents affecting infrastructure hosted by a third party cost small businesses £106K on average, while large enterprises lost nearly £1.5M as a result of breaches affecting suppliers they shared data with, and saw another £1.2M in expenditures because of insufficient levels of protection from providers of Infrastructure as a Service (IaaS) (Ashford, 2017). The threat environments had changed, with hacking software and hackers themselves becoming much more advanced in both capability and reach. Cyber terrorists had progressed in more economically-focused directions including industrial espionage, corporate disinformation, market and financial manipulation, and disruption of critical public and private infrastructures. They had done so without slowing their previous activities such as data exfiltration, system ransom and extortion, and digital vandalism. Mitigating these threats had required businesses to re-think the cybersecurity and business risk postures. In many cases, organizations developed a more inclusive approach to enterprise risk management. Current thinking in business strategies had required companies to reconsider how cyber risks affected the company as a whole, including stakeholders like customers, partners, suppliers, industry groups, and regulators. The

ComputerWeekly.com article quoted Alessio Aceti, head of the enterprise business division at Kaspersky Lab, a multinational Internet security and anti-virus provider, who stated (Ashford, 2017):

> *While cyber security incidents involving third parties prove to be harmful to businesses of all sizes, their financial impact on a company had the potential to result in twice as much damage.*

Because cybersecurity had been considered a business risk as well as a technology risk, integrating monitoring for both of these risks into the company's cybersecurity risk management program had become essential. Cyber risks had impacted entire businesses operationally and financially, and seriously damaged their reputations in the process. In such situations, businesses needed to continue evaluating, updating, and communicating their cybersecurity policies, practices, business rules, training programs, and other procedures to cause the requisite cultural changes required for better cybersecurity hygiene. When done in a holistic way, cyber risk management had become a strategic weapon for better protecting the company's environment while maturing its cybersecurity capabilities at the same time. Companies had approached this challenge by creating better new rules of engagement with their interconnected business partners, such as contractual agreements in which both the company and its partners were required to improve their cybersecurity programs and provide ways to demonstrate the maturity of the programs. However, this change had not been adopted widely, and many businesses had not started to collaborate with their partners in this area. A key reason was that businesses had not had technologies that enabled them to communicate securely with their internal and external stakeholders to deal with mutual cybersecurity risks.

In its 2016 Global 1000 survey, CGI, a leading independent information technology and business process services firm, found that organizations that viewed security not only as a mandatory part of operations, but also as an enabler to growth and change, maximized the benefits of digital transformation efforts. At the same time, only 14% of clients who responded to the Global 1000 survey stated that they were at a level of maturity where cybersecurity was a key part of their value propositions (CGI, 2016). In order to move forward, companies had begun to take input from regulatory, industry, consumer, and other stakeholder groups in order to mature their cybersecurity strategies and risk management systems. By approaching cybersecurity as a business problem first, companies had been better able to create more resilient operational frameworks that would improve their abilities to identify, respond to, and remediate cyberattacks and mitigate any business interruptions more quickly and cost effectively.

Cybersecurity Standards Problems

Cybersecurity practitioners had reviewed security and control-related guidelines and standards to determine which ones of the various government, industry, and independently developed guidelines would be the best ones for them to utilize as they continued development on their cybersecurity programs. Companies had been increasingly challenged by regulators, industry groups, and business partners to become savvier in the areas of maturing their cybersecurity programs and understanding their cyber risks. However, as determined by a review of the academic literature (Fulford, 2017), there were a significant number of cybersecurity and risk management frameworks used by cybersecurity practitioners that ranged from rudimentary ones based on manual questionnaires using qualitative techniques to those that were very complex utilizing strong quantitative and statistical measures. In January, 2018 the IT Governance web site published a review of the most frequently adopted cybersecurity frameworks (Watson, 2018):

- Payment Card Industry Data Security Standard (PCI DSS) – 47%
- International Standards Organization (ISO) 27001/27002 – 35%

- Center for Internet Security (CIS) Critical Security Controls – 32%
- National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Security – 29%

While all of these frameworks had large numbers of adopters, the newer NIST Cybersecurity Framework (NIST CSF) successfully combined qualitative and quantitative methods in an easy-to-use and understandable format. This methodology, which was created in part from the older NIST 800 series security and risk management approach, was found to map directly to most of the control requirements and most of the other security frameworks, which would make it relatively easy to implement for many companies and government agencies. To many companies, the ability to measure and understand cyber risks on several levels internally and externally had become daunting challenges to companies' enterprise risk management programs. A framework, like the NIST CSF, that enabled companies to assess each other's cyber maturity and define collaboration in disseminating ways to better deal with risks across their business ecosystem, regardless of industries involved or the technologies they used to interconnect and exchange products, services, and--most importantly--information.

Current directions in cyber risk evaluation had been seeking a way for companies to "get credit" for the work they were doing to mature their cybersecurity programs while simultaneously identifying cyber risks and related security control gaps. This type of approach had helped senior executives rationalize their investments in their technology footprints and attendant cybersecurity governance and management practices. An overarching cybersecurity implementation and risk management methodology which enabled companies in different industries and business practices to have common vocabulary and taxonomy for discussing and understanding their cyber risks would be extremely beneficial to a variety of industry and government organizations.

Such a methodology had assisted companies in standardizing and streamlining the implementation of cyber risk management controls that were required by the establishment and operation of new business technology interconnections. This had helped businesses to eliminate redundancies in security controls and to increase the understanding of how effectiveness of those controls was measured. Companies had a duty to be more cyber mature, including improving understanding the cyber risks related to their internal and external technology interconnections, as well as their indirect interconnections (such as the interconnections of their business partners' partners).

References

Ashford, W. (2017). *Third-party cyber security failures cost businesses the most.* Retrieved from https://www.computerweekly.com/news/450429441/Third-party-cyber-security-failures-cost-businesses-the-most

Fulford, E. (2017). What factors influence companies' successful implementations of technology risk management systems? *Muma Business Review, 1*(13), 157-169. Retrieved from http://pubs.mumabusinessreview.org/2017/MBR-2017-157-169-Fulford-TechnologyRisk.pdf

The global impact of huge cyber security events. (2017). Retrieved from https://www.helpnetsecurity.com/2017/10/02/impact-huge-cyber-security-events/

The global risks report 2018. (2018). Retrieved from http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

Hutcherson, K. (2018). *Six days after a ransomware cyberattack, Atlanta officials are filling out forms by hand.* Retrieved from https://www.cnnCNN.com/2018/03/27/us/atlanta-ransomware-computers/index.html

Lipson, H. F. (2002). *Tracking and tracing cyber-attacks: Technical challenges and global policy issues.* (No. CMU/SEI-2002-SR-009). Carnegie-Mellon University Software Engineering Institute, Pittsburgh, PA. Retrieved from https://resources.sei.cmu.edu/asset_files/specialreport/2002_003_001_13928.pdf

Soha systems' survey reveals only two percent of it experts consider third-party secure access a top priority, despite the growing number of security threats linked to supplier and contractor access. (2016). Retrieved from http://www.marketwired.com/press-release/soha-systems-survey-reveals-only-two-percent-it-experts-consider-third-party-secure-2125559.htm

Sorcher, S. (2017). *What keeps cybersecurity experts up at night?* Retrieved from https://www.csmonitor.com/World/Passcode/Passcode-Influencers/2017/0327/What-keeps-cybersecurity-experts-up-at-night

Walters, R. (2018). *Federal cyber breaches in 2017.* Retrieved from https://www.heritage.org/cybersecurity/report/federal-cyber-breaches-2017

Wasserman, R. (2010). *Building communities of trust.* Retrieved from https://nsi.ncirc.gov/documents/e071021293_BuildingCommTrust_v2.pdf

Watson, M. (2018) *Top 4 cybersecurity frameworks.* Retrieved from https://www.itgovernanceusa.com/blog/top-4-cybersecurity-frameworks/

Biography

Ed Fulford is an executive in risk, information security, and compliance. He has more than 25 years of international experience assessing, building, and managing IT Security and Risk Management programs for companies such as CGI, CAPCO, RBS WorldPay, Fundtech Corporation, Cingular Wireless, and British Telecom. Fulford earned a Bachelor of Science in Business Administration from the University of Florida and a Master of Business Administration from Troy University. His professional certifications include the Payment Card Industry Professional, Certified Information Security Manager, Certified Information Systems Security Professional, Certified Fraud Examiner, and Certified Information Systems Auditor credentials.