Draft: 7/10/24

Cybersecurity (H) Working Group
Virtual Meeting
May 29, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met May 29, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Bud Leiner (AZ); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Tia Taylor (GA); Daniel Mathis (IA); C.J. Metcalf (IL); Shane Mead (KS); Mary Kwei (MD); Jake Martin (MI); T.J. Patton (MN); Martin Swanson (NE); Tracy Biehn (NC); Colton Schulz (ND); Christian Citarella (NH); Gille Ann Rabbin (NY); Matt Walsh (OH); David Buono and Sebastian Conforto (PA); Rebecca Rebholz (WI); and Lela Ladd (WY).

1. Heard a Presentation from Coalition on the "Effectiveness of Security Controls: A Meta Analysis"

Amann opened the meeting by discussing the planned 2024 presentations on cybersecurity and staying informed of related market trends. She thanked Sezaneh Seymour (Coalition) and Daniel Woods (Coalition) for taking the time to present, noting the high caliber of their important and relevant work.

Seymour expressed how the cyber insurance landscape is changing and how cyber insurers have become a more central part of the security conversation. She said Coalition approaches cybersecurity risk with an active insurance model. Its data suggests policyholders experienced 64% fewer claims than the market average, consistent over the previous few years. Seymour said the evolution of cyber insurance has grown to be more than just a mechanism to transfer financial risk—cyber insurance has become a market-based tool to drive security improvements across businesses and infrastructure. She said Coalition has a team of security experts available to provide technical assistance throughout the policy's life cycle.

Woods began presenting the research by highlighting the key understanding that while cybersecurity is a mainstream national security issue, cyber risk science is difficult. He stated that Coalition's systematic academic literature review reveals an immature body of research. Woods said the research he conducted shows that cyber insurers are beginning to produce evidence not available in scientific literature. They looked at academic and industry research to identify common threads, one of which was the importance of patch management. One study by Gallagher Re found that the speed at which patches are applied is the most important technical predictor of the likelihood of suffering a claim. Woods said the study noted that revenue and industry are still the most important, but when it comes to technological controls, patch cadence seems to be the most important.

The second finding identified multi-factor authentication (MFA) as a highly effective control for protecting individual accounts. Woods said that one outside study identified a 99% reduction in compromise of individual accounts, while another study conducted during the same period found that implementing MFA was associated with the lowest reduction in claims likelihood compared to 10 other controls. The Marsh study sourced questionnaires filled out by clients looking to buy cyber insurance; however, self-reported information continues to be unreliable because a simple "yes" or "no" response is not enough information. Woods highlighted the Change Healthcare incident, wherein the organization had MFA in some places but, for whatever reason, did not apply it to its corporate virtual private network (VPN). Coalition is trying to innovate by taking steps to move away from a checkbox questionnaire insurance application form.

The third important control is attack surface management, which is essentially how organizations configure web infrastructure with which attackers can interact. A key insight is that the revolution of the internet was connectivity, as it created many economic opportunities through connections. When viewed from a security

 

perspective, it creates problems because, in theory, a threat actor could interact with them and potentially compromise security. Attackers can probe any part of the organization's attack surface, and there is no single attack surface to close down. Coalition found that businesses with internet-exposed remote desktop protocols (RDPs) are two-point-five times more likely to file a claim. Ransomware gangs exploit this protocol because it essentially is designed for support, allowing someone from the outside to have total control over the device.

The final control or area of concern is what is referred to as perimeter products or boundary devices. Coalition found one corporate VPN associated with a five-times increase in claims frequency. If a cyber actor can find a vulnerability in one of these types of devices, they could compromise many different organizations with the same type of device on the network.

Seymour provided reflections for state insurance regulators; the research has provided data-driven epiphanies of the obvious, which are to reduce the attack surface, patch cadence, and deploy MFA. Each of these is likely to move the needle with respect to an organization's security. Seymour emphasized how this type of research would not have been possible even several years ago because cyber insurers have only recently started to make this data available. She further explained that Coalition recognizes a bespoke approach to cyber insurance is required to accurately measure and effectively mitigate cyber risk. Seymour concluded the presentation with several observations and recommendations for consideration. First, she said that Coalition encourages the option to rate without filing, and where that is not an option, approval timelines need to accelerate dramatically. Second, it encourages state insurance regulators to keep the mutually reinforcing nature of cyber insurance and security services in mind, allowing insurers to offer discounts when policyholders implement risk reduction measures. Third, in the context of ongoing work on data privacy, it encourages being mindful that the goals of transparency and data minimization do not inadvertently undermine ongoing threat research and information sharing in the cybersecurity space.

Chou opened the question-and-answer (Q&A) period by providing a high-level review of the relationship between the regulatory body and the role the filing process plays in securing and addressing solvency concerns, specifically encouraging the industry to work together to discuss when any state's response is too slow, or they may identify opportunities for accelerating the review process.

Amann inquired about insurers putting requirements on client companies to implement risk reduction measures and whether Coalition has received pushback on the matter. Seymour explained how they evaluate a potential new policyholder through a risk assessment, resulting in a risk profile category. Coalition does not require policyholders to have perfect security, but it reserves the right to make coverage contingent on the policyholder correcting any critical vulnerabilities identified. Woods provided additional insights into the resources of its policyholders, which are mostly small businesses, explaining that they do not have the ability to manage 3,000–4,000 vulnerabilities each month. The Coalition team works to identify the vulnerabilities most likely to be exploited by threat actors and sends those notifications to their clients, guiding insurance toward the most effective interventions. Amann opined that state insurance regulators should develop something along the lines of the National Institute of Standards and Technology (NIST) framework for some regulatory expectations of what insurers are required to do.

Unal Tatar (University at Albany) asked a question about what impact Coalition sees government initiatives in software vendor liability having or will have on reducing the risk level for buyers and an impact on cyber insurance. Woods responded with a personal view from an academic perspective. He explained that when an organization adopts Cisco, it has a particular product with a 500% increase in the probability of having a cyber insurance claim. This is where software liability could be relevant because the policyholder probably had no idea when they bought the product five years prior. The assignment of liability by state insurance regulators could be interesting because the vendors essentially need to be held accountable for building insecure software. This accountability is what

 

motivated the discussions at the federal level. Woods suggested there is a role for insurers to segregate against those vendors given the kind of increased information available. Seymour reflected on how today's burden for security, in software and misconfigurations, is disproportionately placed on the end users of those technologies. The system in which the insurance world is navigating is often the consumers who are the least placed to secure technology. In order to shift the burden, it is important for the organization to effectively manage controls like limiting attack surface and patching cadence.

Chou asked Woods to provide more information regarding the patch management example in the presentation material, wherein the vulnerability and patch were published Oct. 10, but a week after, threat actors were detected to be exploiting the vulnerability. Chou asked whether some users have not updated their systems and how it can be prevented if that is the case. Woods explained how many organizations are not fully resourced and ready, which could have avoided this incident. If a system administrator is applying to a crucial VPN enabling remote employees to continue working, if there is an error in doing so, it could lead to all of those employees not being able to produce work for a day. System administrators want to test and ensure the patch is reliable, which is something Coalition is attempting to address through prioritization.

Peter Kochenburger (Consumer Representative) asked for an example where legislation or regulation is designed to increase transparency and reduce the amount of data needed to the absolute minimum. Woods described how the legal interpretation of attorney-client privilege and work product doctrine applies to digital forensics investigations. Specifically, how some investigations are found to not be protected by privilege because they are not conducted for the purpose of advising lawyers. He noted that some digital forensics firms stop writing down incident investigations, which means those findings cannot be used to advocate for improvements after the incident to share threat intelligence.

Schulz asked about a list or a database of minimum standards that could be used by information technology (IT) examiners to see that companies are meeting the minimum standards. Seymour and Woods provided information on the machine learning (ML) system at Coalition that scores vulnerabilities from the national vulnerability database. Organizations should look to patch the vulnerabilities with a higher score, prioritizing the ones most likely to be exploited.

Peterson explained how cyber insurance covers unusual risk, as it is much more dynamic, and asked how the presenters generally predict the industry evolving. He further asked if Coalition thought that in the future, the people who write insurance policies will also be the same people doing gap analysis. The speakers jointly described how insurers are likely going to need to either partner with security service providers or become one themselves. Woods remarked that carriers cannot just sell a PDF for peril, adding that the sale must be alongside security.

Diederich asked the speakers to discuss the challenges posed by legacy systems or the bespoke in-house applications, some of which may be old and not currently patched. Woods described how some of the critical sectors, like health care, might have legacy systems running on Windows XP and how the recommendation would be for them to take those systems offline, partly because security is not a product so much as it is an ongoing process and requires active care.

Having no further business, the Cybersecurity (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Summer/WG-Cybersecurity/Minutes-CyberWG052924.docx