Cybersecurity at MIT Sloan

During COVID-19, are you Adequately Protecting Against Cyber Threats?

Summary of the content presented by Michael Coden, and Ron Ford during the 3/27/2020 CAMS Friday Meeting

As millions of staff move out of offices to work from home using new remote-work communication technologies, the company's attack surfaces increase. Simultaneously, cyber criminals are using COVID-19 fears and the ensuing chaos to take advantage of unsuspecting people. In this CAMS Friday Research Team meeting, **Managing Director of BCG Platinion Global Cybersecurity and CAMS Research Affiliate Michael Coden** shared research done by his team on how companies and their workforce can respond to these new threats from the COVID-19 environment. In addition, **Ron Ford, Regional Cybersecurity Advisor-New England at the Department of Homeland Security (DHS)** described how the DHS is perceiving these new threat areas and how they are tackling uncharted risk.

"COVID-19 and cybersecurity are similar in that patching your computers is like washing your hands, and not clicking phishing emails is like not touching your face."

The Attack Surface has Increased Signifigantly

As the pandemic moves forward, society's focus on the health and human aspects of COVID-19 have taken priority over cybersecurity concerns; however, cyber criminals' focus continues to be on ways to disrupt, hack and make money. All workers, but especially remote workers, must be more vigilant than before so they do not fall prey to these new vulnerabilities. Since many workers have never worked from home, they may not realize that both their work and there personal digital connections are being targeted. This could impact both the workers and their families. Cybercriminals are targeting home networks of C-suite execuitves to get access to corporate at-home endpoints—this is the broader attack surface- the increase in end points open to hackers. Many companies have not ventured into the space of protecting workers homes from attack, but they must consider these end points as new vulnerabiliites to the corporate systems.

Security techniques that work inside physical offices may no longer be effective, and the security team may not be ready to manage the broader range of environments that remote work introduces. One way to manage risk is to limit when employees have access to systems and data. By limiting access to work hours to the regular work day, software will detect a criminal trying to hack into systems in the middle of the night. Another tactic is to separate personal and work networks. Using different networks for different computers will ensure that work computers will not be able to 'speak' to a family member's computer, potentially cutting off a channel for hackers to access.

Authentication

Authenticating who is calling for support adds another layer of vulnerabilies in a remote work environment. When workers call from a known phone number, such as the phone in their office, the IT help desk can easily authenticate the source of the call. But when workers work from home, and use their personal phone to seek help, the help desk must authenticate a different way, and those mechanisms may not have been set up prior to the pandemic. Add to that the speed by which workers were sent home to work, and it's just about guaranteed that the help desk is left trying to validate callers in whatever way they can. New systems may need to be put in place quickly to assure manual authentication is successful.

Phishing and the Human Element

Phishing has also taken a nasty turn during the pandemic as hackers are praying upon email user's intentions to respond to urgent needs and clicking on links inside emails without thinking about the possible threat. Coden suggested a good rule of thumb is to not click on any links about COVID-19. If necessary, type the URL into a search engine directly to be sure it's a valid destination and not altered to go to a hacker's site.

The insider threats may increase, too. In an office, coworkers are less likely to copy files to an unauthorized disk or transfer them to an inappropriate destination for fear of being seen. When the 'cops' aren't around, employees might not be as careful to stick to the rules or they may not even consider their actions as something that breaks the rules. With many meetings taking place online, it's impossible to prevent someone from taking a screen shot of corporate information on their webinar screen or sharing insider information in their home environment. Finding ways to minimize these threats is another need.

Cybersecurity and Infrastructure Security Agency's (CISA) Efforts to Curtail Threats Related to COVID-19

DHS Advisor Ron Ford shared his agency's view. CISA's worldwide Threat Assessment Report from Jan 2019 warned that adversaries and strategic competitors will increasingly use cyber capabilities- including cyber espoionage, attacking, and influencing, to seek political, economic, and military advantage over the United States. CISA is working closely with partners to prepare for potential cybersecurity impacts of a COVID-19 outbreak in the United States especially as the activities will rely heavily on healthcare and first responder systems and include potentially damaging information that must be kept cybersecure. CISA has published several reports with assessments and suggestions for cybersecurity impacts from the pandemic. Visit https://www.cisa.gov/insights for the latest reports.

"Pandemic" has been added to the modern risk landscape when it comes to Cyber Security. One of the best practices suggested by CISA during situations like the COVID-19 crisis is to have specific leadership own the issue. When leaders openly, directly and confidently lead their team through increased cyber threat, it creates confidence within the team and an environment based preparedness and responsibility. Additional suggestions from CISA include increase focus on good cyber hygiene (like patching software and securing devices) and reviewing business continuity plans to be sure they are appropriate for the the current environment.

About Cybersecurity at MIT Sloan

Cybersecurity at MIT Sloan brings together thought leaders from industry, academia, and government with MIT faculty, researchers and students to address strategy, management, governance and organization of cybersecurity of critical infrastructure using an interdisciplinary approach.

For more information, visit https://cams.mit.edu

RESOURCES SHARED IN THIS MEETING

- Ron Ford, DHS, slide deck: https://cams.mit.edu/wp-content/uploads/CISACybersecurityCOVID-19BriefRonFord2020.pdf
- CISA website on Coronavirus (and critical infrastructure considerations): https://www.cisa.gov/coronavirus
- CISA Cybersecurity Recommendations during COVID19 Website: https://www.cisa.gov/insights
- Michael Coden, BCG, slide deck: https://cams.mit.edu/wp-content/uploads/BCG_COVID_Cybersecurity_MCoden_March2020.pdf
- BCG Report: Managing the Cyber Risks from Remote Work During COVID19: https://www.bcg.com/publications/2020/covid-remote-work-cyber-security.aspx