Lessons Learned
from the
2020
ICIT FALL BRIEFING
Secure Roadmap
for the Future

FEBRUARY 2021

BUILDING A HOLISTIC CYBERSECURITY CULTURE

Authored By:
Drew Spaniel, Lead Researcher, ICIT

Contributors:
Joyce Hunter, Executive Director, ICIT & Former Deputy CIO for Policy & Planning, USDA
Janet Vogel, CISO, HHS
Jothi Dugar, CISO, NIH
Venice Goodwine, CISO, USDA
Sherry Bennett, PH.D., Chief Data Scientist, DLT Solutions

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

DLT
A TECH DATA COMPANY

According to the 2020 Verizon DBIR, (Data Breach Investigations Report) there were 3,950 confirmed breaches in 2020. The onset of the COVID pandemic resulted in a drastic increase in exploitable vulnerabilities, phishing attempts, ransomware campaigns, and remote compromise attempts. Nevertheless, an estimated 40% of organizations did not have a comprehensive cybersecurity strategy that leveraged technical and non-technical controls to secure their networks and assets and promote cyber-hygiene best practices amongst their workforces. At the 2020 ICIT Fall Briefing, ICIT Executive Director Joyce Hunter moderated a panel featuring leading CISO's perspectives on how to best cultivate and propagate a holistic cybersecurity culture throughout an organization.

Cybersecurity Remains a "People Problem"

Holistic cybersecurity is a measure of your understanding of the organization and your ability to leverage your insights into actions. Jothi Dugar, CISO NIH, explained that holistic reform had to begin by listening to staff, learning about the organization's deficiencies and needs, and understanding the cybersecurity posture with respect to the threat landscape. At its core, cybersecurity remains a "people" problem. She offers, "In cybersecurity, we tend to try to tackle things at the superficial level to put "band-aid fixes" on it. Instead, we should look at it from a holistic standpoint, of people, process, and technology. We need to empower our people with the knowledge, skills, tools, and resources that they need to understand their role in security and embed security into their roles." Janet Vogel, CISO, HHS agrees, adding, "Cybersecurity isn't one thing, it's everything. It's in everything we do. And because we're so connected right now, in so many ways, we need to think about cybersecurity as a part of our daily life."

Business Drives Cyber, But Education Ensures Adoption

Venice Goodwine, CISO USDA, explained that in many organizations, "business drives cyber," so it is productive to put initiatives in those terms. For instance, she explained that when COVID-19 spread, business continuity relied on a transition to telework. USDA, which operates at over 4,500 locations globally, had to educate its personnel to adapt to secure telework quickly. Educational efforts included cybersecurity best practices such as connecting securely and how to secure their BYOD systems. It also included cyber-hygiene best practices such as detecting suspicious behaviors, identifying phishing attempts, what to avoid when working from home, etc. The education initiative succeeded because her team conveyed the important information in brief handouts designed to maximize comprehension and adoption. Additionally, to offset negative behaviors that arose from frustration or anxiety, USDA ensured that help desk infrastructure was continuously available to provide assistance whenever needed.

Gamification Improves Engagement and Retention

Ms. Goodwine confided that the key to long-term cultural reform is to constantly remind staff of cybersecurity and cyber-hygiene best practices in various ways that reinforce their vigilance against emerging threats. Ms. Vogel agrees and explains that HHS increased the retention of their cyber-hygiene curricula by experimenting with gamification and different mediums such as crossword puzzles, cartoon caption contests, and other activities that broke from the monotony of annual training. Ms. Goodwine adds that USDA experienced similar positive results with gamification exercises like escape rooms and trivia contests that appealed to younger members of the workforce but were still accessible to older generations. She explains, "Really vary your approach to learning because it gets everyone excited about the cybersecurity you try and incorporate within the organization. That cybersecurity is everyone's business, and you're going to have to use varying methods to engage them. You have to meet them, 'where they are' because maybe they are generationally different and what works for them may not for their peers. So, we augment the standard training, to reach multiple people in different ways." It also helps to design exercises to challenge how people think and expand their depth of thought. For instance, someone who thinks visually may learn from more verbal material, or someone who is non-technical may benefit from technical experiences. Growth comes in many forms, and the foundation is often challenge and conflict. Gamifying educational efforts and gearing them towards different ways of thinking expands the staff's minds' elasticity and enables them to recognize different threat vectors or types of cyber adversary more easily.

Engage People's Senses

Ms. Dugar explains that people learn and increase their wellness through the incorporation of sensory input. Playing a cybersecurity game may work for some based solely on the thrill of the game, but, for others, additional incentives such as food or rewards may increase engagement and enhance the experience. Even just verbal and auditory stimuli can be engaging if it is an active dialogue that engages participants. Dr. Sherry Bennett, Chief Data Scientist, DLT, suggested, "Dynamically adjust and think consciously about how you deploy new strategies in terms of your training and outreach to people. Create alignment among leadership and communicate that down to everybody about new activities that might expand risk and discuss the types of actions we need to take."

Allow Breaks to Refocus, Recoup, and Retain

Phishing attempts to prey on apathy, stress, and momentary lapses in vigilance. In addition to stimulating sensory engagement, personnel must take breaks to allow their brains to passively interpret, process, and incorporate information so that it can be retained in the long-term. With the migration to telework, a short break with a pet or completing a short household task can increase the serotonin and dopamine that facilitate mental wellness. Small expressions of control over our work environment, such as a daily tidying regiment or a separation from the home space, can decrease stress, increase attention and focus, and combat the depression and "cabin fever" that many experienced after transitioning telework. Ms. Bennett recommended setting a weekly social call for the team to connect without the pressure of work deadlines and projects. These experiences emulate the normal social interactions we expect from our workplace that were lost to the telework transition.

Leverage Technology to Do What People Can't

Improving the behaviors of the workforce will not mitigate every threat. Worse, Ms. Vogel explains that as budgets are decreasing, information security teams are being asked to do increasingly more with fewer resources. Efficiently mitigating risk is a matter of cost savings. Ms. Hunter stated, "Where we cannot educate personnel to improve their cyber-hygiene and cybersecurity practices, we can strategically incorporate technology." Ms. Bennett recommended incorporating user behavioral analytics, identity and access management, and machine learning solutions to monitor activity, log actions, improve personnel behaviors, and mitigate attempted compromises. She also suggests that organizations consider emerging threats and their technical and non-technical strategies to combat threats holistically. Threat actors should be considered according to their motives, methodologies, and capabilities. She also recommends that we anticipate what the enemy is thinking about from a holistic perspective regarding the political landscape, cultures, and current events, like the COVID-19 pandemic.

Conclusion

Building a holistic isn't necessarily a matter of investment or resources. It is more about educating personnel and strategically empowering them to learn, grown, and retain the information. By weaponizing the workforce to be vigilant against emerging threats, resources can then be allocated towards the gaps that the workforce cannot reasonably monitor or secure. By better incorporating cybersecurity and cyber-hygiene best practices throughout the average workday activities, leaders can institute a holistic cybersecurity culture that actively and iteratively improves the organization's security posture.