FEATURE

It's Time to Stop Today's Cybersecurity Insanity

You may have heard the adage, "Insanity is doing the same thing over and over again and expecting different results."[1] Often misattributed to Albert Einstein or other geniuses, its genesis was a 1981 Narcotics Anonymous pamphlet. How apropos, as most of today's cybersecurity programs rely on concepts developed in the 1980s and early 1990s. To use a 1980's phrase, "You'd have to be delusional" to believe a 20th century approach to cybersecurity would be effective in today's 21st century hyperconverged cyber environment!

Sadly, many organizations continue to practice their own special version of cyber insanity, investing heavily in revamped versions of stale technologies and then wondering why they continue to be the victims of cyber attacks and incidents.

Gregory J. Touhill, CISM, CISSP
Is a retired US Air Force Brigadier General and current president of the Cyxtera Federal Group, which offers market-leading data center services and cybersecurity capabilities to US federal agencies and departments via a portfolio of secure infrastructure solutions delivered from a global footprint of world-class data centers, including six in the Washington DC, USA, metropolitan area. Prior to joining Cyxtera, Touhill was appointed by US President Barack Obama as the nation's first-ever federal chief information security officer in 2016, where he was responsible for ensuring that the proper set of digital security policies, strategies and practices were adopted across all US government agencies. He currently serves on the ISACA® Board of Directors. He can be reached at *https://twitter.com/cyxtera* and *https://www.linkedin.com/in/gregorytouhill/*.

Cybersecurity is big business, with some think tanks estimating cybersecurity spending will rise nearly 10 percent and hit almost US $100 billion in 2018. Spending in both public and private sectors on antivirus software, virtual private networks (VPNs), intrusion detection, monitoring and other traditional cybersecurity technology to safeguard data continues to rise amidst fears of data breaches, ransomware, and attacks from cyber criminals and nation-state actors. These increases indicate that boards of directors and senior executives recognize the need to invest in better protecting the information that fuels today's national prosperity and national security, even global economic growth, yet these very same leaders are becoming increasingly frustrated. Many express that with all their spending on cybersecurity tools, one would think their organization would perform much better than they actually do. To be fair, many organizations have improved, yet I contend that we are underperforming and should do much better at a lower cost to protect our information, our intellectual property, our brands and reputation, and our competitive advantage.

Many boards and senior executives ask me for help. They want to reduce their cyber risk and, while most express suffering from "cyber spending fatigue," they are not shy about investing more resources as long as they show a good return. Nearly every organization I work with has laser-like focus on fixing their "cybersecurity problem" through the purchase of another tool or technology. Focusing on technology alone to fix a problem reminds me of what US Airmen call "target fixation," where you get so fixed on one thing that you do not recognize the threats around you, resulting in a crash or getting shot down. Cybersecurity involves people, process and technology, yet too many practitioners focus on technology and ignore people and process. To stop the insanity, we need to look beyond solely spending on another tool and first invest in building a cybersecurity culture that balances people, process and technology to improve our ability to manage cyber risk.

Without an effective cybersecurity culture, your organization is fighting a losing battle. Gustavo Grodnitzky, Ph.D., makes the case that by focusing efforts on supporting the behaviors and performance we seek, we will develop the culture we desire.[2] When it comes to cybersecurity, I agree with Dr. Grodnitzky: "Culture trumps everything!"

> "TRADITIONAL CYBERSECURITY PROGRAMS KEEP SPENDING AN INSANE AMOUNT OF MONEY ON REHASHED VERSIONS OF 1990S TECHNOLOGY AND EXPECTING THEIR CYBERSECURITY POSTURE TO IMPROVE."

When I was the US government's chief information security officer (CISO), a member of the US Congress asked me how I would spend another US dollar on improving cybersecurity. I told him that I would spend it to improve our cybersecurity culture. I believe our policies are adequate yet are poorly executed. For example, Edward Snowden "borrowed" US National Security Agency (NSA) administrator credentials from some of his peers in violation of policies, leading to his theft of highly classified information. The US Office of Personnel Management (OPM) was victimized by bad actors using compromised user name and password credentials despite policy requiring multi-factor authentication identity and access management. Similar examples in the private sector are plentiful, such as when bad actors breached Equifax by leveraging unpatched known vulnerabilities. The best policies, tools and technologies are worthless without a healthy cybersecurity culture where everyone in the organization has a solid understanding, acceptance and employment of their roles in protecting information.

Recently, ISACA® and the CMMI Institute examined how well their members and customers believe their organizations are making progress toward developing and adopting a cybersecurity culture. The 2018 ISACA/CMMI Culture of Cybersecurity Research sought to determine whether there is a gap between the desired and current states and how organizations are seeking to bridge any gaps that exist. A "cybersecurity culture" within an organization is defined in the survey as the behaviors and habits that stem from a defined set of policies for data handling, cybersecurity, risk

Dr. Grodnitzky's model of cultural components serves as a useful construct to assess the findings of the 2018 ISACA/CMMI Culture of Cybersecurity Research regardless of where in the organization you are. His model cites behavioral norms, habit patterns, connectedness, trust, language and time perspective as critical components of culture. While you likely may append others to your personal cultural framework, these are great starting points for discussion:

- **Behavioral norms**—Essential elements of every cybersecurity program. If you are not able to identify what you want done and what your standards are, you greatly increase the risk of failure.
- **Habit patterns**—Essential to building a solid culture. Habits are the intersection of knowledge, skill and desire.[3] To make something a habit, you need the knowledge of what to do and why, the skill to know how to do it, and the motivation to do it.
- **Connectedness**—An essential cultural component that describes the condition where members of an organization believe they have a sense of belonging, ownership or community.
- **Trust**—An important part of any organization is the belief that the person or entity you are dealing with will behave in a way that demonstrates reliability, responsiveness, capability and personal interest. In my opinion, a Zero Trust security model is warranted to best manage cyber risk.
- **Language**—Critical to the success of any organization. A shared common language increases activity, profit, efficiency and cybersecurity, while fostering connectedness and trust.
- **Time perspective**—An important cultural element that reinforces behavior. Rewards for good behavior and penalties for unacceptable behavior need to be applied quickly.

tolerance, and other sets of cultural norms and practices that reflect on both individuals and the entire enterprise. More than 4,800 respondents shared their thoughts, perceptions and experiences to questions that gauged topics that touch upon issues affecting all stakeholders, from senior executives to frontline practitioners.

There are numerous instructive golden nuggets in the survey, and one highlights the critical need to stop the insanity of today's current practice of chasing the latest technological fad and instead focusing on improving cybersecurity culture. Traditional cybersecurity doctrine prioritizes senior leadership buy-in as the critical component leading to successful cybersecurity programs. While I agree that it is a vital component, the survey clearly indicates that the greatest factor inhibiting organizations from achieving their desired cybersecurity culture is employee buy-in. The usual suspects of lack of funds, goals, tools, leadership, talent, etc., all fell below lack of employee buy-in when determining whether you will achieve your desired cybersecurity culture.

Traditional cybersecurity programs keep spending an insane amount of money on rehashed versions of 1990s technology and expecting their cybersecurity posture to improve. That insanity has to stop. As one of the US government's former senior cyber operators, I know hackers, cyber criminals and nation-state actors easily defeat traditional security gear, especially when it is paired with a careless, negligent, indifferent or poorly trained workforce. Twentieth-century cybersecurity approaches are not good enough in today's environment. You do not have to be a genius to see that now is the time to invest first in building a strong cybersecurity culture throughout your organization and secure employee buy-in. Only then can you pair your well-informed and motivated workforce with modern and secure 21st century tools and architectures to better manage and control cyber risk. To do otherwise is just plain crazy.

Endnotes

1 Narcotics Anonymous, World Service Conference of Narcotics Anonymous Basic Text Approval Form, Unpublished Literary Work, USA, 1981, chapter 4, p. 11
2 Grodnitzky, G.; *Culture Trumps Everything: The Unexpected Truth About the Ways Environment Changes Biology, Psychology, and Behavior*, Mountain Frog Publishing, USA, 2014
3 *Ibid*.