A Fairy Tale of Innovation

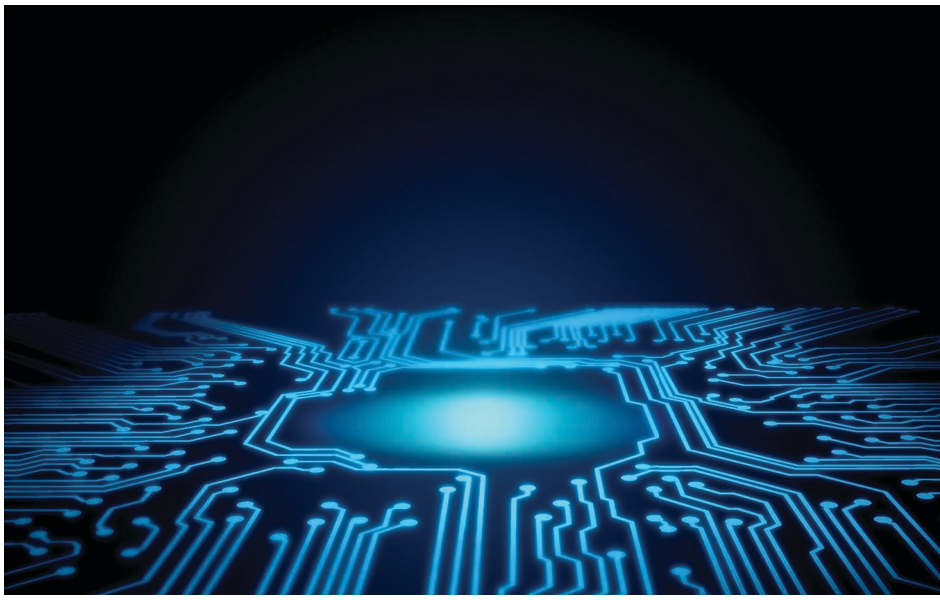
Greetings traveler! Since you have been navigating the wonderful and informative world of the *ISACA® Journal* for some time, you have likely been inspired to explore and question the world around you. I invite you to take a break from staring at screens for I have a tale to tell. One that invites you to consider a different world, the seemingly magical devices we use every day and the fabric that connects them to each other. You see...

Once Upon a Time...

...There were pirates and cowboys in cyberspace. Men and women seeking their futures and fortunes in an untamed digital landscape that had yet to be touched or changed by mankind. Forging ahead and making names for themselves as great pioneers and adventurers, they manifested new devices and software into existence. These new discoveries interested not only academics and technologists, but slowly caught the eye of the general public as the new technologies helped make life slightly easier with each new innovation.

Huge strides such as the home PC, the Internet and, eventually, the smartphone paired with cellular technology brought all of these conveniences not just to our fingertips at home or in the office, but anywhere in the world. With the mass adoption of these devices came the building of the backend infrastructure to house large data sets and processing power, which spawned the next digital revolution in innovation. This also was the starting point of accelerating technologies such as the Internet of Things (IoT), artificial intelligence (AI) and cloud. However, during this global digital transformation, there was another mythical character lurking in the shadows—the dreaded wizards (also known as hackers).

These villains sought to exploit vulnerabilities and overlooked coding and security errors in new products for their own benefit and educational gain. Posing as regular players in this fairy tale kingdom by day, at night they played with forbidden magic such as scanners and fuzzers to circumvent protocols and bend devices to their will, and, in doing so, gained unauthorized access, leaving the organization's reputation, controls and policies in shambles. Sometimes these intruders would send sys admins and coders information on what they found, how they exploited it, and even at times how to fix it, but they did not have explicit written permission to do so and, therefore, would be punished for their curiosity. However, some organizations, realizing the benefit of these practices, offered these wizards jobs to help



Dustin Brewer, CISM, CSX-P, CDPSE, CEH
Is ISACA's senior director emerging technology and innovation, a role in which he explores and produces content for the ISACA® community on the utilization benefits and possible threats to current infrastructure posed by emerging technologies. He has 17 years of experience in the IT field, beginning with networks, programming and hardware specialization. He excelled in cybersecurity while serving in the US military and, later, as an independent contractor and lead developer for defense contract agencies, he specialized in computer networking security, penetration testing, and training for various US Department of Defense (DoD) and commercial entities. Brewer can be reached at futures@isaca.org.

Enjoying this article?

- Read *The Pulse: Emerging Technology 2021. www.isaca.org/go/emerging-tech-2021*
- Learn more about, discuss and collaborate on emerging technology in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

them discover these vulnerabilities and fix them. And some of these wizards traded robes and staffs for khakis and polo shirts. And, thus, cybersecurity was born.

The Allegory of the Cybercave

Of course, this is just a cross-genre, silly and overly simplified interpretation of the history of the Internet and cybersecurity. Silliness aside, the extreme speed and leaps we have made in technological innovations in the last 50 years are astounding and noteworthy. This innovation is so fast, in fact, that humanity is having a hard time keeping pace with it. Despite advancements in technology, cyberattacks are on the rise with no end in sight.[1] The support from senior leaders for adopting emerging technologies is there, but there is hesitation[2] because implementing any technology into current infrastructure brings with it the possibility of increasing cyberattack surfaces and possible vulnerabilities. In other words, it is hard to implement new and emerging technologies while we are still trying to secure traditional infrastructure, and there seems to be little hope in sight.

It was recently pointed out to me that when I talk about emerging technologies, I tend to speak more to the history of the technology. While this may seem counterintuitive at first, every forward leap we make in innovation is weighed down by the fact that the underlying security of devices does not improve. In a fairy-tale world, I would say that this exemplifies the fact that humans are doomed to repeat history. The more practical explanation is that past behaviors often predict future ones. Without true change in the way we use and secure technology, we are likely to continue our current trends.

And, once again, there is the interconnectivity between technology and humanity. As the old adage says, end users are the weakest part of any network. The more I dive into emerging technology and cybersecurity, the more I realize how silly this statement is. Not because it is not true, but because humans or end users are the only reason networks exist in the first place. As IT practitioners inundated by technology on a daily basis, it is easy to lose sight of that. In a fairy-tale world, we would defeat the security issues that plague our networks and make the world safer for emerging technology implementations by throwing the one ring of vulnerability into the fires of Mount Doom, thus ending the reign of possible exploitation. But, of course, this is not a fairy tale. In real life, this change will take time and effort to be successful, but all too often we try to look for the one thing to fix it all. The truth is that to secure our older technologies and create space for the new ones to grow will take effort, patience and understanding to teach all users—whether C-suite or customers—the importance of governance, risk assessment, cybersecurity and IT.

> "IT IS HARD TO IMPLEMENT NEW AND EMERGING TECHNOLOGIES WHILE WE ARE STILL TRYING TO SECURE TRADITIONAL INFRASTRUCTURE."

Endnotes

1 ISACA®, *State of Cybersecurity 2021, Part 2: Threat Landscape, Security Operations and Cybersecurity Maturity*, USA, 2021, *https://www.isaca.org/go/state-of-cybersecurity-2021*

2 ISACA, *The Pulse: Emerging Technology 2021*, USA, 2021, *https://www.isaca.org/go/emerging-tech-2021*