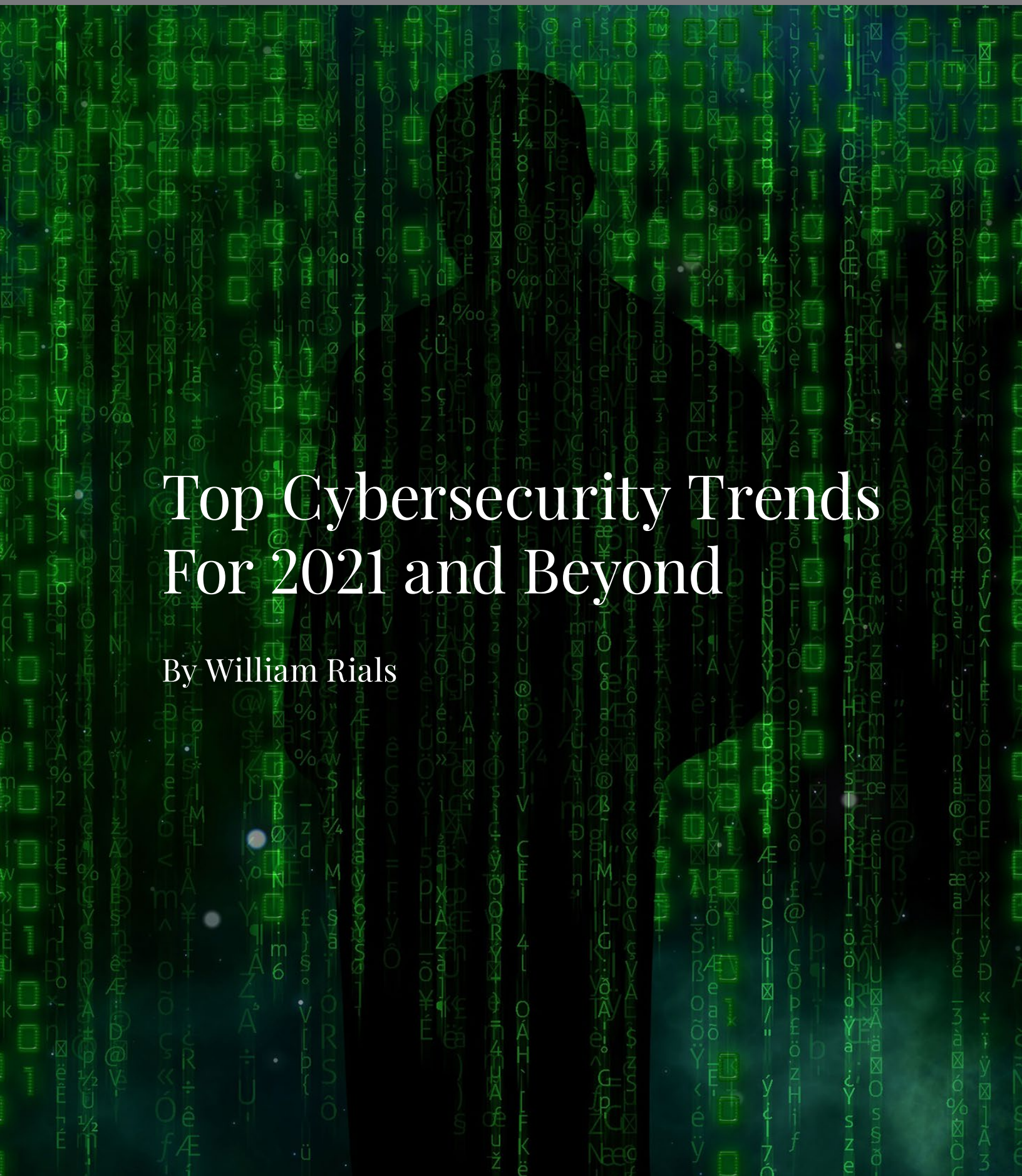

Top Cybersecurity Trends For 2021 and Beyond

By William Rials

Abstract

This article provides an overview of the cybersecurity landscape and how it was dramatically shifted due to the COVID-19 pandemic. In addition, it provides a look into the future with the top 10 cybersecurity trends and predictions for 2021 and beyond. The pandemic response caused massive disruptions to the way we live, work, and conduct business. Organizations rapidly shifted to online operations and remote working to maintain normalcy during the pandemic. These transitions will continue into post-pandemic and beyond as the new normal. Cybercriminals have responded and will use this opportunity to launch a new breed of cyber attacks in 2021. The article outlines the top cybersecurity concerns for 2021 and beyond.

Suggested Citation

Rials, William. "Top Cybersecurity Trends for 2021 and Beyond."*Homeland Security Affairs: Pracademic Affairs* 1, Article 3 (May 2021). www.hsaj.org/articles17153

Introduction

Along with every other discipline, the cybersecurity threat landscape was completely disrupted in 2020 due to the pandemic. The COVID-19 pandemic was a central theme last year and caused significant disruptions in the way we utilize technology to conduct business. The response to work-from-home and lockdown orders forced organizations to reconsider how and where they conduct business and cybercriminals took advantage of increased remote work and cloud adoption.

Holistically, organizations have become security conscious and have taken an initiative to increase their defense against threats. Cyber Awareness campaigns have been successful in increasing basic cyber hygiene practices. National campaigns such as the Cybersecurity and Infrastructure Security Agency's "Stop, Think, Connect"[1] and the National Initiative for Cybersecurity Education (NICE) have produced positive cybersecurity industry outcomes. However, the pandemic and the rapid shift to remote, online, and cloud services have disrupted not only 2020 but also the future cybersecurity trends in 2021.

I have been in the technology industry for 20+ years and specializing in cybersecurity for most of my career. I have graduate degrees in technology and cybersecurity, and my Ph.D. dissertation research involved cybersecurity and cloud computing. Currently, I am utilizing my skills, expertise, and experience as a professor of practice and associate program director for Tulane University's technology and cybersecurity programs. Additionally, I am active in many national-level cybersecurity organizations as a subject matter expert. As such, I typically receive emails and requests for "What is coming next for cybersecurity?" and "What are my cybersecurity predictions for the upcoming year?" Due to the technology response to the pandemic last year, I believe that in 2021 we will still be in a biological pandemic but also a Cyber Pandemic.[2] The evolving business and IT landscapes have created new cyber exposures and increased

attack surfaces. The volume, range, and types of cybersecurity attacks will potentially be vastly different next year. Below are my Top 10 Cybersecurity Trends for 2021 and beyond. Although every cybersecurity threat identified in this report should be considered significant, the threats are ranked in order of priority and potential risk levels, starting with the highest risk items first.

Cybercriminals Will Continue to Exploit The Pandemic for Cybersecurity Attacks

During 2020, we saw a 600% plus increase in COVID-19-related cybersecurity attacks.[3] This trend will continue in 2021 as the pandemic will be at the top of everyone's minds and on news coverage. Continual news of vaccine developments or new national restrictions will cause phishing attacks to increase throughout the year. Attackers will look to seize the opportunity to exploit the keen interest in the ongoing pandemic and will continue to exploit this public interest to gain a foothold in target systems. Pandemic social engineering attacks in 2021 will likely focus on government-issued stimulus checks and vaccine information. Criminals have worked quickly to take advantage of the vaccine rollout to trick users into clicking on malicious links in emails and SMS messages. Since the pandemic began, there has been a 300% increase in cybercrime.[4] The FBI is already tracking social engineering attacks that utilize the public's interest in the COVID-19 vaccine. [5] In 2021, cybercriminals will use the pandemic to their advantage, and we will see an even larger increase in cybercrime.

Home Offices Will Be Top Cyber Targets

The boundaries between home and office blurred last year, and cybercriminals realize that home offices are not only easy targets but accessible gateways into the corporate network. Work will continue to be performed over home internet connections. Many home routers lack advanced security features and remain unpatched and even outdated. In 2021, we will see increased attacks on home networks. Cybercriminals will begin to use home network devices as launching pads to attempt to gain access to other higher targets. The most extensive vulnerabilities will be exploited on home internet routers and connected Internet of Things (IoT) smart devices.

Additionally, with more employees working from home, cybercriminals will focus on vulnerabilities in personal computers, especially the software and operating systems. As a pandemic response, over 80% of organizations allowed employees to use personal devices. However, over 70% did not have adequate security configurations and lacked enterprise malware protection, and relied on the basic software included with the endpoint device.[6] It is essential to reflect that the rise in remote work is happening during the same year Microsoft has ended support and stopped issuing security updates for Windows 7, which is still the most popular home operating system. Hackers will seek to exploit the increasing flaws in Windows 7 because many home users will not easily update their devices. I predict that at least one major corporation will suffer a cyber breach due to a corporate employee's home network.

Ransomware Will Remain A Top Threat

Ransomware has increased 239% since 2019, and it is nothing new to learn that ransomware was near the top of many security threats lists in 2020. In 2021, it is not surprising to anticipate that ransomware attacks will only continue to increase. The ransomware damage costs are predicted to be $20 billion USD of the overall $6 trillion USD caused by cyber incidents by 2021. A business will fall victim to a ransomware attack every 11 seconds at that time,[7] and the cost to recover from a ransomware attack has increased by 228%.[8] Ransomware attacks will continue to evolve to become even more technically advanced by using Advanced Persistent Threat (APT) techniques to explore, probe, and map the entire network to locate the most valuable and vulnerable systems before starting the enterprise-wide encryption. The new breed of ransomware will change administrator accounts before the final attack and utilize blitz attacks to encrypt multiple devices simultaneously. The new variants of ransomware will also encrypt and destroy data, threaten to leak potentially compromising data, and put additional pressure on victims to pay ransom fees. A common strategy to mitigate the risks associated with ransomware has been to keep a copy (backup or primary) of the data in a cloud file sharing service. In 2021, we will see ransomware attacks expand to cloud data shares as well as on-premises hard drives.

The Rapid Shift to Cloud Will Expose Security Risks

The pandemic caused organizations to quickly pivot to cloud services, online business, remote work, and home offices. The deployment of these emerging technologies like cloud and online operations was implemented at a rate never seen, and this trend will continue into next year. Experts predict cloud deployments to increase by over 35% in 2021.[9] Unfortunately, many of these services were implemented with security as an afterthought. While the quick pivot to cloud-everything did enable operations to continue functioning during the pandemic and extended the organization's borders, it also introduced many new security risks. More importantly, most new cloud deployments were implemented with default configurations or improper settings for fast and easy use. Many of these misconfigurations are still in place, and hackers will exploit these vulnerabilities. Virtually every high-profile cybersecurity breach with a cloud deployment was due to misconfigurations caused by the inexperienced cloud end-user. Even veteran IT professionals need additional skills and training to configure and secure cloud resources properly. The responsibility of where the cloud service provider's responsibility ends and the organization's responsibility starts is often misunderstood by new users of expanded cloud services. Many new cloud adopters make the incorrect assumption that cybersecurity is the complete responsibility of the cloud service provider.[10]

In 2020, we saw threat actors take advantage of these insecure cloud deployments, but the majority of hackers have only done footprinting and recognizance exercises. In 2021, we will see a plethora of cloud security holes exposed and organizations compromised due to the rush to cloud in 2020. Enterprise applications and cloud software implemented will be continually hounded by hackers. The rapid acceleration of cloud adoption during the pandemic will shift the cybersecurity landscape dramatically.

The primary issue is that traditional IT methods cannot respond to the speed and agility of the cloud, and IT professionals and end-users alike have more power than ever in their hands with the cloud. Additionally, cloud infrastructure is growing in complexity requiring specific skillsets. Because of the ease of availability, many IT professionals are experimenting with public cloud services without fully understanding the complete details from a security perspective. This vastly increases the overall risk profile. Virtually every security breach involving data hosted in public clouds exposing information or other critical assets was caused by incorrect configuration by humans. The common mistake is that most organizations still use traditional IT tools and techniques to manage cloud security and compliance. Cybersecurity has traditionally been based on physical security concepts. I have often used the example of a medieval castle to explain traditional cybersecurity methods. The purpose of a castle was to keep the people and contents on the inside safe. The defenders would build strong high walls, towers, a moat, and other layered perimeter defenses. The castle defenders would build a drawbridge to control and limit the access into the castle's interior from a single point. This is like cybersecurity professionals installing a firewall and IPS/IDS at the network border and control ingress/egress to the protected assets inside the network. This type of security architecture is fundamentally at odds with today's cloud and edge architecture. Applying tried and true traditional cyber defense methods will not be successful in the new computing beyond the perimeter wall in an edge-computing environment.

Vulnerabilities Targeting 5G Connected IOT Devices will Increase

The completely connected, fast digital reality promised by 5G also gives cybercriminals more access and opportunities to launch attacks targeting all devices connected to the new 5G network. As 5G networks begin to be implemented nationwide, the numbers of connected IoT devices will also immensely expand, considerably increasing 5G-connected network vulnerabilities to large-scale, multi-vertical cyberattacks. Botnets and Distributed Denial of Service (DDOS) attacks have reduced somewhat in recent years due to emerging cyber defense technologies. However, the 5G expansion will fuel the botnet armies and increase attacks.

Implementing ways to secure 5G effectively will be a concern in 2021, and the quality and integrity of the IoT devices themselves will continue to be a threat next year. Cybersecurity professionals are looking at new IoT devices' internal workings for signs of implementation problems, cryptographic discrepancies, and even backdoors.[11] Hackers will perform their own testing on legitimate IoT devices to look for undiscovered vulnerabilities that they can exploit. I predict that we will see several high-profile IoT-related hacks in 2021.

Legacy Technical Architecture Will Be The Weak Link for Many Organizations

Any legacy technology, including servers, network infrastructure, workstations, and especially software applications, have always been prime targets for threat actors. These legacy devices and endpoints are usually not maintained as much as modern deployments. In many cases, the original vendor no longer supports or provides updates and patches to the legacy equipment. In these cases, vulnerabilities will go unmitigated for long periods of time, allowing hackers easy access. The focus during 2020 was all about the response to the pandemic and for remote access. Many projects to upgrade legacy systems were put on the back burner because the pandemic response took priority. Vulnerable legacy systems remain at corporate offices. This, combined with the fact that most employees will continue to work from home with equally or more outdated technology, is a cybersecurity disaster recipe. One glaring example is Windows 7 and Server 2008 operating systems. Specialized hardware and legacy equipment also prevent many organizations from upgrading away from legacy operating systems because the underlying equipment is not compatible with the newer operating systems. A significant portion of business and home users will continue running outdated and legacy operating systems that are long past their expiration dates. Cybercriminals will see this as an opportunity and look for ways to take advantage. I expect that we will see several new vulnerabilities surface that will result in significant security breaches as hackers will ramp up targeting these legacy systems.

In addition to the legacy endpoints, many organizations rapidly deployed legacy security architecture to deliver virtual operations and remote as soon as possible. Some of these examples included allowing Remote Desktop Protocol (RDP) sharing through the corporate firewall and legacy Virtual Private Network (VPN) services. In contrast, these services make for fast and easy deployments and configuration for remote services. It also comes with serious security risks, and even novice-level hackers can easily exploit these types of configurations.[12] With more than 400 million businesses using these services, we will likely see an increase in VPN and RDP attacks during 2021.[13]

Social Engineering Attacks Will Increase and Become More Sophisticated

For years, social engineering has been one of the top tools in the hacker's toolbox. Webroot describes social engineering as the art of manipulating people, so they give up confidential information.[14] This is usually done with carefully crafted emails or text messages tricking victims into clicking on a malicious link. The malicious links may contain malware or take the user to a website for more advanced social engineering tactics to gain access to passwords or other sensitive information. Social engineering attacks account for more than 80% of reported security incidents. [15] Organizations can have a healthy security posture, but social engineering methods involve deceiving users into unknowingly breaking the standard security practices. With over 50 million social

engineering attacks, nearly 90% of all organizations worldwide experienced a social engineering attack within the last year.[16] The volume of cybersecurity social engineering attacks will exponentially increase in 2021. In addition to the number of social engineering attempts, the sophistication of the attacks will increase as well. Email filters have matured and use technologies to identify and block social engineering and phishing emails. Cybersecurity user awareness campaigns have increased, as has end-users' knowledge of how to spot suspicious emails as phishing attacks. Criminals will continue to modify their attacks in response to the defense measures. Social engineering attacks in 2021 will be challenging to identify by both email filters and human perusal.

Emergence of Cybercrime Gangs

Criminals working together to commit crimes is not a recent phenomenon. Criminals have had a long history of joining together to commit organized crimes. Traditionally, hackers and cybercriminals have worked independently or in smaller groups. Threat actors have been quite segmented, specializing in one type of malicious hacking activity. Last year, we started to see the beginnings of cybercriminal organizations collaborating and even coordinating attacks. Some cybercrime groups are coming closer and closer together. One example is ransomware developers working with botnet operators. A recent threat assessment report said the popular malware variants of Emotet, Trickbot, and Ryuk are now so close that they should belong in the same group. They have become more competent at working together.[17] I believe that this type of collaboration between cybercrime groups forming into organized cybercrime gangs with a formalized hierarchy of leadership and strategic plans enacting advanced, simultaneous attacks will be a common theme in the future.

Outside-Out Architecture and Focus on Users

Due to the cloud, virtual, and remote expansion of 2020, the future state of Information Technology will see an increased expansion in Shadow IT. Shadow IT environments will continue to proliferate throughout an organization's enterprise as the employees or groups within a department will explore and find new ways to work around enterprise IT restrictions. Cloud and Software-as-a-Service make it easy for end-users to bypass enterprise systems and spin up their own environments. These environments are loosely monitored and provide expanded attack surfaces for cybercriminals. Along with Shadow IT, the increased usage of mobile devices such as smartphones, tablets, and IoT devices all represent network devices that are increasingly difficult to secure, and most end-users are constantly connected via multiple devices.

We will see a cybersecurity architecture focus evolution from IT assets to user analytics, access, and authentication during the following year. Historically, cybersecurity has primarily focused on securing technology components, such as databases, processes, services, hardware, network infrastructure, and other devices. However, if the end-user remains the weakest link in the cybersecurity chain, I predict more emphasis on identity and access management will become the future trend. With modern cloud deployments, most organizations' data and critical assets are outside the traditional network perimeters, and end-users are on a separate outside network.

As Development and Operations (DevOps) have become mainstream, the future trend will be Development, Security, and Operations (DevSecOps). DevSecOps will focus on the user and privileged access management to resources wherever they are located. Advanced technologies, such as AI and intelligent authentication, will ensure that the specific end-user will have the appropriate level of authentication to a digital asset at the correct time. A global leader in Privileged Access Management, BeyondTrust, refers to this emerging security practice as Identity-Centric Security.[18] Regular business and technology will continue to move out of the traditional, on-premises environment. Security defense measures will focus more on the proof of identity rather than securing network devices.

Maintaining Operational Balance In The New Normal

These cybersecurity threats and trends identified should be balanced with the increasing demand for continuous delivery of valuable business services in a disruptive technology environment. The year 2021 will usher in a new norm of doing business and utilizing technology. The focus of cybersecurity issues in 2021 and onward should evolve from a control mindset into a governing mindset. Cybersecurity professionals will govern access to resources, especially user privileged access. They will work out ways to achieve the business's desired outcomes versus locking everything in the network down.

About the Author

Dr. William (Bill) Rials is the Associate Director and Professor of Practice of the Tulane University School of Professional Advancement Information Technology and Cybersecurity Program, where he focuses on continually delivering and updating the program curriculum based on innovative and emerging technologies. In addition to the responsibilities of running the program, Dr. Rials is also a Professor of Practice and a Distinguished Faculty Member where he teaches innovative technology undergraduate and graduate classes. He is a nationally recognized subject matter expert on information technology. He has had a career as an IT executive with broad experience delivering value to government, academic, and business partners through the innovative use of technology. He was recently named a senior fellow at the Center for Digital Government. The Center for Digital Government (CDG) Senior Fellows are experienced and respected state and local government practitioners and scholars who have demonstrated records of success in support of public service. Dr. Rials had a diverse government technology career delivering value to state agencies, local governments, and law enforcement agencies throughout the state and local government space. He has served in CIO, CTO, and CISO roles for local governments and also in various leadership positions within the State of MS IT organization as a deputy to the State CIO. In this role, he crafted the blueprints for the state's first hybrid cloud strategy and served as chair of the statewide Chief Information Officers (CIO) council. His government technology leadership was recognized in 2015 when he was elected Vice-President of the National Association of State Technology Directors (NASTD) southern region; he was later asked to serve as president in 2016.

In 2017, he was given an award as one of the top 50 IT government professionals in the Nation by States Scoop magazine. Additionally, he continues to serve as the principal consultant and Chief Technology Officer (CTO) for a technology managed service company specializing in delivering cloud and cybersecurity solutions to small businesses. Dr. Rials' military service was with the MS State Guard where he completed Officers Candidate School conducted by the MS Military Department. His military service included working with the National Guard Assistant Chief of Staff (ACoS) G6 Office performing cybersecurity analysis and training for staff as well can a commander for a military police company. He was awarded the emergency service medal by the Adjutant General (TAG) of the MS National Guard for his service in leading the MP company that was in charge of the joint force headquarters security detail during hurricane Isaac in 2012. Dr. Rials holds a bachelor's degree in business administration from Belhaven University, a master's degree in Computer Information Systems and Cybersecurity from Missouri State University, as well as a Ph.D. in higher education administration and public administration from Jackson State University. His dissertation research involved the critical factors that affect the adoption of cloud services within the public sector. He is a noted expert in the IT and Cybersecurity space and frequently quoted by national media outlets. He is also a frequent contributor to national IT government organizations such as NASTD, NASCIO, and the Center for Digital Government. He may be reached at brials@tulane.edu .

Notes

1. "STOP. THINK. CONNECT. ™," Cybersecurity and Infrastructure Security Agency (CISA), accessed March 10, 2021, https://www.cisa.gov/stopthinkconnect.

2. Robert O'Brien, "The Next Global Crisis: A Cyber Security Pandemic," MetaCompliance, September 15, 2020, https://www.metacompliance.com/blog/the-next-global-crisis-a-cyber-security-pandemic/.

3. "Coronavirus-Related Spear Phishing Attacks See 667% Increase in March 2020," *Security Magazine RSS* (Security Magazine, April 15, 2020), https://www.securitymagazine.com/articles/92157-coronavirus-related-spear-phishing-attacks-see-667-increase-in-march-2020.

4. Jenna Walter, "COVID-19 News: FBI Reports 300% Increase in Reported Cybercrimes," *IMC Grupo*, May 2, 2020, https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes/.

5. "Federal Agencies Warn of Emerging Fraud Schemes Related to COVID-19 Vaccines," FBI (FBI, December 21, 2020), https://www.fbi.gov/news/pressrel/press-releases/federal-agencies-warn-of-emerging-fraud-schemes-related-to-covid-19-vaccines.

6. "Bring Your Own Device," *Total Cloud Security*, https://pages.bitglass.com/cd-fy20q3-bringyourowndevice_lp.html.

7. Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," November 13, 2020 *Cybercrime Magazine*, January 22, 2021, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

8. Elizabeth Gow Content Creator, "Must-Know Ransomware Statistics for 2021," EMPIST, January 9, 2021, https://empist.com/must-know-ransomware-statistics-for-2021.

9. "Forrester Predictions 2021 - Read All Forrester Predictions For 2021," *Forrester*, accessed March 10, 2021, https://go.forrester.com/predictions/.

10. John Edwards, "7 Steps to a Well-Architected Cloud," *CIO* (March 20, 2019), https://www.cio.com/article/3373837/7-steps-to-a-well-architected-cloud.html.

11. Authors GReAT et al., "Advanced Threat Predictions for 2021," Securelist English Global securelistcom, https://securelist.com/apt-predictions-for-2021/99387/.

12. Liam Tung, "VPN Warning: REvil Ransomware Targets Unpatched Pulse Secure VPN Servers," ZDNet (ZDNet, January 6, 2020), https://www.zdnet.com/article/vpn-warning-revil-ransomware-targets-unpatched-pulse-secure-vpn-servers/.

13. GWI, "VPN Usage Around the World Infographic," GlobalWebIndex, https://www.globalwebindex.com/reports/vpn-usage-around-the-world.

14. "What Is Social Engineering? Examples And," *Webroot*, 2019, https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering.

15. Josh Fruhlinger, "Top Cybersecurity Facts, Figures and Statistics," CSO Online (CSO, March 9, 2020), https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html.

16. "State of the Phish," State of the Phish, Proof Point, 2020, https://www.proofpoint.com/sites/default/files/gtd-pfpt-uk-tr-state-of-the-phish-2020-a4_final.pdf .

17. "Internet Organized Crime Threat Assessment," Europol, 2020, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020.

18. Person, "Top Cybersecurity Trends Tor 2021: The Hacking of Time, M/L Data Poisoning, AI Attacks, & More," BeyondTrust (BeyondTrust, October 23, 2020), https://www.beyondtrust.com/blog/entry/top-cybersecurity-trends-to-watch-in-2021.

Copyright

Copyright © 2021 by the author(s). Homeland Security Affairs is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of Homeland Security Affairs or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in Homeland Security Affairs rests with the author(s) of the article. Homeland Security Affairs is the online journal of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS).
Cover image by tigerlily713 from Pixabay.