March 2022

ICIT 2022
SPRING BRIEFING
PRIMER

PLAYING TO WIN

Using Strategy to Create Your Cybersecurity Battleplan

Authored By:
Drew Spaniel, Lead Researcher, ICIT

Contributors:
David Wray, ICIT Fellow and Strategic Program Manager, MFGS, Inc.

ICIT Institute for Critical Infrastructure Technology
The Cybersecurity Think Tank

MFGS INC. Micro Focus Government Solutions Master Supplier | MICRO FOCUS

Playing to Win

Using Strategy to Create Your Cybersecurity Battleplan

March 2022

ICIT would like to thank the following organizations for supporting this objective, vendor-agnostic, non-partisan research:

MFGS, Inc.

ITG

CyberRes

Carahsoft

Contents

Introduction:

Securing US critical infrastructures and democratic institutions requires whole-of-government vigilance, dedicated leadership, and strategic innovation. In many ways, cybersecurity is an asymmetric tower-defense war game where a digital fog of war obfuscates numerous adversaries with unpredictable resources and varying tactics. Organizations begin with the certainty that their systems will be targeted and an accounting of the resources at their disposal to attempt to mitigate attacks or remediate breaches. Proactive strategic planning that incorporates emerging data in real-time and adapts to evolutions in the threat landscape is essential to deter adversaries and mitigate disruptive incidents. However, many organizations fail to recognize the need to modernize their reactive strategies into proactive approaches or adopt a modern strategy altogether. As in physical conflicts, the responsibility of rallying the defense and routing oncoming attackers falls to leaders capable of anticipating adversarial efforts and communicating a comprehensive strategy. This publication will acclimate cybersecurity thought-leaders on how to develop and implement effective and proactive strategies.

Wins and Losses: 2021 Lessons Learned Defending National Security

Prolific events such as the SolarWinds breach, exploitation of the Log4J vulnerability, and the Colonial Pipeline attack have increased discussions around the importance of cybersecurity. There have been at least a dozen high-profile software supply chain exploits leveraged en masse by adversaries over the past five years, according to the National Counterintelligence and Security Center (NCSC). Some of these incidents, infamous by the name of the vulnerability exploited or malware deployed, include NotPetya, GoldenSpy, ShadowHammer, and SolarWinds/BlueOrigin [1]. Software supply chain attacks exploit vulnerabilities present in popular applications and code at any development lifecycle stage to grant adversarial access, conduct espionage, or enable sabotage. Adversarial tools and tactics vary in degrees of sophistication; however, many of the popularizing attack paradigms focus on exploiting tools, dependencies, libraries, third-party code, and infrastructure that is common across many potential critical infrastructure targets. Prolific attacks on the software supply chain have highlighted the need to:

- Better assess vulnerabilities in the people, processes, technologies, and code on which the security of US critical infrastructure depends. Gamification, improved insider threat policies and solutions, and expanded secure information sharing can help improve organizations' ability to recognize exploitable vulnerability and mitigate the risk.
- Recognize what can be securely and strategically automated and what operations require direct management. Judicious use of digital workers, a security-centric remote work policy, and clear and inclusive communication of the security strategy to all stakeholders can help organizations maximize the security potential of their networks, systems, and personnel.
- Reduce the organization's attack surface by better understanding networked devices, underlying code, third-party and partner security, and the value of assets. Zero trust frameworks, comprehensive security, risk assessment, and incident response plans, and proactive and deliberate, long-term strategies can improve the security posture of organizations and their critical assets.

Meanwhile, current events, such as the Russia-Ukraine conflict at the time of this writing regularly rekindle vigilance around potential APT attacks. So far, though, words have been louder than action.

Greater resources are necessary to modernize legacy systems and secure public and private critical infrastructure against emerging threats and attack vectors. There is also a need to update how we operate and recognize positive change. The past few years have consistently stressed that organizations need to prioritize cybersecurity as a business driver and essential rather than relegate it to an afterthought. Further, organizations need to update their internal cultures and embrace changes that might empower them to invest in their cybersecurity more readily or improve their personnel's knowledge, capabilities, and continuous learning. Though the transition to remote work introduced its security challenges, some organizations significantly enhanced their ability to recruit and retain domestic STEM talent by hiring outside their geographic location. Burnout and mental fatigue of cybersecurity staff were also decreased with the transition to remote work as daily commutes were reduced and the adoption of automation solutions, such as digital workers, increased. Though cyberattacks increased during the past year, as detailed below, the optimistic outlook is the hope that organizations now better understand which assets are mission-critical and how to secure those systems according to their value.

The federal government has likewise not been idle. CISA, NIST, and other agencies have ramped up proactive efforts to improve public-private information sharing, secure organizations against emerging threats, and promote national security and resiliency. In response to the surge in supply chain attacks last year, President Biden issued Executive Order 14028, "Improving the Nation's Cybersecurity." According to CISA's summary of the Executive Order, it:

- Removes Barriers to Threat Information Sharing Between Government and the Private Sector
  - The EO ensures that IT Service Providers are able to share information with the government and requires them to share certain breach information.
- Modernizes and Implement Stronger Cybersecurity Standards in the Federal Government
  - The EO helps move the Federal Government to secure cloud services and a zero-trust architecture and mandates multifactor authentication and encryption deployment within a specific period.
- Improves Software Supply Chain Security
  - The EO will improve software security by establishing baseline security standards for the development of software sold to the government by requiring developers to maintain greater visibility into their software and making security data publicly available.
  - It also creates a pilot program to create an "energy star" label so the government – and the public at large – can quickly determine whether software was developed securely.
- Establishes a Cyber Safety Review Board
  - The EO establishes a Cyber Safety Review Board, co-chaired by government and private sector leads, with the authority to convene following a significant cyber incident to analyze what happened and make concrete recommendations for improving cybersecurity. This board is modeled after the National Transportation Safety Board, used after airplane accidents and other incidents.
- Creates Standardized Playbook for Responding to Cybersecurity Vulnerabilities and Incidents
  - The EO creates a standardized playbook and definitions for cyber vulnerability incident response by federal departments and agencies. The playbook will ensure all federal agencies meet a certain threshold and are prepared to take uniform steps to identify

and mitigate a threat and serve as a template for the private sector to coordinate response efforts.
    - Improve Detection of Cybersecurity Incidents on Federal Government Networks.
    - The EO improves the ability to detect malicious cyber activity on federal networks by enabling a government-wide endpoint detection and response (EDR) system and improved information sharing within the Federal Government.
- Improves Investigative and Remediation Capabilities
    - The EO creates cybersecurity event log requirements for federal departments and agencies to improve an organization's ability to detect intrusions, mitigate those in progress, and determine the extent of an incident after the fact.

Notable 2021 Cybercrime Trends and Outcomes

Adversaries capitalized on the chaos and tumult caused by the COVID-19 pandemic by exploiting the nascent points of network ingress and egress that arose from the rapid migration to distributed workforces and some increased targeted attacks against third party entities in attempts to laterally compromise critical supply chain systems [2]. Supply chain attacks have been on the rise since the Sunburst cyber-espionage campaign, which initiated an approach that resulted in successful campaigns on software producers and cloud service providers such as SolarWinds, MS Office 365, etc., and followed the methodologies demonstrated by seven similar events from the last decade. During the Solar Winds breach in 2020, hackers exploited the configurations of the Orion NMS software and inserted malware into SolarWinds's servers, which was packaged as part of an update. This effectively allowed the threat group to gain access to systems of any organizations using Orion NMS, among which are the US Department of Defense and 425 names in the US Fortune 500 [3]. Meanwhile, sophisticated adversaries have not been idle. FireEye estimates there are currently ~2000 distinct hacking groups, including nation-state-sponsored threat actors (known as APTs), financially motivated groups (known as FINs), and uncategorized groups (known as UNCs) [4]. Across industry, Check Point Research estimated that attacks from adversaries of all degrees of sophistication increased in 2021 (Table 1).

Table 1: Average Weekly Attacks per Organization by Industry (2021)		
Industry	**Average Weekly Attacks**	**% Increase from Previous Year**
Education/Research	1605	+75%
Government/ Military	1136	+47%
Communications	1079	+51%
ISP/MSP	1068	+67%
Healthcare	830	+71%
SI/VAR/Distributor	778	+18%
Utilities	736	+46%
Manufacturing	704	+41%
Finance/Banking	703	+53%
Insurance/Legal	636	+68%
Leisure/Hospitality	595	+40%
Consultants	576	+73%
Software Vendor	536	+146%
Retail/Wholesale	526	+39%
Transportation	501	+34%
Hardware Vendor	367	+16%

Table 1 depicts the average weekly attacks per organization by industry in 2021 based on data from Check Point Research.

It can be challenging to gauge the annual trends in cyber-adversarial behaviors because incidents are often underreported or may not yet be discovered. From the available data, though, we can assert that cybercrime flourished during 2021 because cybercriminals adapted their tools, tactics, and procedures to the shifts in hybrid environments and the threat landscape.

- In their *2021 Evil Internet Minute* Report, RiskIQ estimated that **per minute in 2021** [5]:
  - 648 cyber incidents occurred
    - Losses averaged $1,797,945 per minute in 2021.
      - $29,965.75 every second
    - Cost an average of $7.2 per minute
      - For fields such as healthcare, the impact of breaches is higher, averaging about $13 per minute.
    - Necessitated average cybersecurity spend of $280,060
  - 525,600 records were compromised
  - 6 organizations were victimized by ransomware
  - $3615 was lost to cryptocurrency scams
- In their *2021 Cost of a Data Breach* Report, IBM shares that breaches between May 2020 and March 2021 cost an average of $4.24 million, a 10% from the $3.86 million reported in the previous year's report [2].

- In their publication *Vulnerability and Threat Trends Report 2021: Cybersecurity comes of age*, Skybox found a 106% increase in new ransomware and a 128% increase in new trojans between 2020-2021 [6].
- Between 2020-2021, the FBI measured a 300% increase in reported cybercrimes [7]. Globally, cybercrime is expected to inflict costs exceeding $6 trillion in 2021, and by 2025, the cost is expected to increase to at least $10.5 trillion annually [8].
- Symantec estimated that between 2020-2021, 1 in every 4,200 emails was a phishing attempt [9].
- Verizon's *2021 Data Breach Investigations Report (DBIR)* found that [10]:
    - Phishing was involved in 36% of data breaches, a 25% increase over the previous year's dataset.
    - 80% of hacking-related data breaches resulted from insecure web apps
- National Cybersecurity Alliance asserts that 28% of all data breaches involve small businesses [11].
    - 25% file for bankruptcy following an incident
    - 10% permanently close
- Atlas VPN estimated that 45% of the global fraud attacks that occurred in Q3 2021 involved brand abuse [12]
- In the wake of the disclosure of the Log4J vulnerability in December 2021, Check Point Research found that the number of cyberattacks per week reached 925 per organization monitored [13].

Anticipated 2022 Trends

Based on ICIT's research of threat actor activities, current events, recent significant incidents, and publicly available information concerning developing agency efforts, the following cyberattack trends are predicted for the remainder of 2022.

DDoS May Resurge

For the first time, DDoS attacks breached the 10 million mark for annual attacks in 2020, an almost 1.6 million increase over the 2019 count. NetScout observed that the rate of DDoS attacks started increasing in March of 2020, which coincides with the outbreak of the COVID-19 pandemic. During that period, the month of May saw the most attacks, with 929,000 recorded. At the height of the pandemic and compared to 2019 metrics, attack propensity increased 25% but decreased by 51% in duration. The number of attacks leveraging 15 or more attack vectors increased by 2851% between 2017 and 2020, likely as more vulnerable IoT devices were networked. Sectors most affected by these attacks are e-commerce, online learning, healthcare, and broadband providers. The surge in such attacks can also be attributed to the sudden jump in digitization or reliance on online services for business continuity [14].

With disruptionware and "hacktivist" attacks on the rise, low-sophistication, high-impact attacks like DDoS are primed to surge in 2022. The ability to take an essential website or system offline during a critical period is appealing to attackers intent on sowing chaos or achieving a public impact.

Open-Source Vulnerabilities will be Exploited

Open-source software promises potential savings, especially to small businesses; however, it also carries proportional risk as adversaries can more easily inject flaws into code, detect exploitable vulnerabilities, or fingerprint network-facing systems against known open-source vulnerabilities. Even without considering the costs to mitigate risk or vulnerabilities, open-source adoption by the public and private sectors alike may increase costs significantly in areas such as integration, customization, training, maintenance, etc.

The open-source code libraries leveraged by government and commercial software providers have not fared much better. Areas of high risk may include the open source-based tools for IoC and Software-Defined environments used to build core infrastructure and afford adversaries a common attack surface on which many critical modern applications depend. One promising strategy to mitigate some of the risks that public sector organizations assume when using open source libraries would be to further develop government-wide code repositories that can be leveraged to create government-off-the-shelf (GOTS) applications and custom tools. For example, the Department of Commerce Source Code Policy promotes software code reuse by making custom-developed Federal source code available across the Department and other Federal agencies [15].

Supply chain attacks on open-source software and libraries grew 650% in 2021, according to Sonatype's *State of the Software Supply Chain* report, increasing from 2000 in July 2020 to over 12,000 by the same period of 2021 [16]. Sonatype did note that open-source supply chain attacks began to drop at the start of 2022, likely due to open-source platforms and supply chain organizations both reacting to tighten security; but, it remains unclear whether that vigilance and diligence will stand throughout the year, and it may be disrupted as more organizations consider open-source reliance as a short-term solution to recouping pandemic losses. In their *2021 State of Open-source Security* report, Contrast Security found that [17]:

- While the average application contains 118 libraries, only 38% of libraries are active.
- The average library uses a version that is 2.5 years old—which increases the risk of unaddressed vulnerabilities.
- The average Java application has 50 open-source library vulnerabilities.
- High-risk licenses are present in 69% of Java applications and 33% of Node applications—exposing organizations to significant legal consequences.

A University of Bonn study found that repositories for Node.js (npm) and Python (PyPi) are the primary targets for supply chain attacks, "supposedly due to the fact that malicious code can be easily triggered during package installation." Meanwhile, Sonatype's report assessed the number of vulnerabilities across the most common open-source packages. It found that the Maven Central repository of Java packages had the highest number of components with vulnerabilities, including more than 350,000 deemed 'critical,' meaning that they could be easily exploited to gain root-level access. In second place was the nmp repository for Javascript packages, with 250,000 components with critical vulnerabilities. Table 2 depicts the number of known and critical vulnerabilities detected in popular open-source code libraries.

Table 2: Total Number of Components in Open-Source Packages Found with Vulnerabilities per Library		
	# Components with at Least One Known Vulnerability	# Components with a Critical Vulnerability
Java (Maven)	612,988	356,808
JavaScript (npm)	459,576	250,002
Python (Pypi)	147,994	81,731
.Net (Nuget)	112,031	27,288

Source: Sonatype *State of the Software Supply Chain* Report (2021)

Cybercrime will Continue to Flourish

Cyber attackers are commonly categorized according to their tools, tactics, procedures, attributed motivations, estimated resources, and technical sophistication into groupings that range from nation-state sponsored advanced persistent threat to cyber-criminal to script kiddie. While the actor may occasionally blur between categorizations, the model broadly holds based on their capabilities and motivations. While a nation-state-sponsored advanced persistent threat actor might launch a ransomware campaign or fiscally motivated attack, their ulterior motive is typically geopolitical. In contrast, cybercriminals almost exclusively operate for fiscal gains. The past year featured prolific nation-state attributed APT attacks such as the attempts to compromise the COVID-vaccine supply chain and the breach of SolarWinds; however, it is not yet clear whether there was a substantial increase in APT activity over previous years. Confirmed breaches in the healthcare industry increased by 58% in 2020, and there was a 238% increase in cyberattacks against financial institutions [17]. In their publication *Vulnerability and Threat Trends Report 2021: Cybersecurity comes of age*, Skybox found a 106% increase in new ransomware and a 128% increase in new trojans between 2020-2021 [6].

As long as cybercrime remains profitable, it will continue to flourish and draw new attackers into the threat landscape. Based on prolific media attention of incidents like the Colonial Access pipeline attacks or even just frequent ransomware attacks, there is no indication that cybercriminals would be deterred from continuing attack campaigns or launching new attacks.

Disruptionware is the New Normal

Ransomware is the weaponization of encryption against a target system. In most attacks, the attacker holds critical systems or files hostage until the victim pays the demanded amount. If the victim does not pay, they are forced to either restore their system from an isolated backup, reset it to factory settings, or lose the system entirely in the case of irreplaceable legacy infrastructure. Every minute that the system remains encrypted disrupts operations and costs potential profits. A business falls victim to a ransomware attack every 11 seconds, and a very low estimate of the damage inflicted from ransomware attacks in 2021 was $20 billion [18]. The average cost of a ransomware attack has increased by about 33% annually since 2019 and now sits around $133,000 [19].

Especially with the increase in activity of notable disruptionware-focused APT threats such as the Russian state-sponsored BlackEnergy group, it is exceptionally likely that attacks aimed at rendering systems inoperable via ransomware, wiper malware, cyber-kinetic impacts, or multiple vectors will increase.

MaaS Obfuscates APTs and Elevates Cybercriminals

Malware-as-a-Service is a developing economy on dark web markets that enables low sophistication threat actors to conduct more impactful attacks and high sophistication attackers to either obfuscate their activities amongst lower-level attacks or extract additional resources by selling less current malware. Essentially, threat actors can purchase malware applications, platforms, and software bundles "off the shelf" and deploy malware in targeted or sweeping attacks. Over the past few years, MaaS rose as a malicious foil to the conventions of application development [20]. The malware author sells it at a fixed price and then provides the development, patching, and maintenance of the malware in return for either a percent of the compromised data or ransom or as a subscription or license fee. Because many of the MaaS are "point and click" or "plug and play," the offerings significantly decrease the technological barrier to launch an attack campaign [20]. While the end-user still needs to know how to deliver or deploy the malware, some platforms offer automation features and forums, and sellers are more than willing to provide tutorial instructions.

Devising the Future: Emerging Strategies, Innovations, and Solutions

Executive Order 14028: Improving the Nation's Cybersecurity also inspired agencies and Congress to consider talent recruitment, retention, rotation, and education programs, which are omitted here for brevity but are detailed in the ICIT legislative and agency initiative briefings and reports. Compensation remains low in the public sector compared to the private sector, and by most accounts, federal, state, and local governments are still struggling to recruit and retain cybersecurity talent. Over the past few years, many discussions have focused on retooling requirements or investing in community college training programs. While all those options have their own short-term merits, most of them are focused on adults who have already entered the US workforce in other verticals or may not be in the workforce for more than the next decade. The demands of the cyber talent shortage are greater than what retraining existing workers can meet. Long-term national security can be significantly improved if greater focus were placed on recruiting K-12 students into STEM fields or promoting interest in information security at all levels of academia. Even if those students do not eventually pursue roles in the public sector or even in cybersecurity, the improvement in the nation's foundational understanding of basic cybersecurity and cyber-hygiene principles will help quell the success rate of future attacks. Consider that an estimated 73-97% of cyberattacks still include phishing attempts as a vector in their campaign. Phishing is low resource, high success, and high impact. Attackers rely on it because it continues to work. A whole-of-nation response is necessary to educate citizens to better recognize social engineering attempts, disinformation, or the early hallmarks of nefarious cyber activity [10].

In its October *2021 Cybersecurity Workforce Study* (ISC), [2] reported that the number of global unfilled cybersecurity positions decreased from 3.12 million (2020) to 2.72 million (2021). However, the study found that the cybersecurity workforce gap increased in every global region except the Asia-Pacific region, which still had a workforce gap of 1.42 million [21]. At the time of this writing, the American cybersecurity workforce numbers at around 1,053,468 according to CyberSeek, a project supported by NIST's National Initiative for Cybersecurity Education (NICE). While that may seem impressive for a nation of around 330 million, the US has an additional 597,767 cybersecurity job openings that remain unfilled [22]. More simply, based on just the numbers at the time of this writing, only 68% of US cybersecurity positions are filled. Estimates for how many additional cyber professionals will be needed

by 2025 vary, but most predictions lie in the range of one to three million additional positions. Worse, many of those currently employed in US cybersecurity may consider retirement within the next decade or leave the field if compensation falls too low. The nation might be in desperate need of cyber-defenders during the pinnacle of digital warfare. The worst time to need fresh cyber talent is after attackers are already digitally assaulting your infrastructure. Thought leaders need to plan ahead and leverage every tool available to develop strategies to recruit and retain cyber talent.

Novel Tools of Education, Training, and Workforce Improvement

In addition to evolving how organizations appreciate cybersecurity and attract talent, leaders should consider the technical and non-technical resources that can help them better recruit, train, and retain talent. Tools that make training more interactive, such as gamification, increase cybersecurity and cyber-hygiene training attention, internalization, and retention. Meanwhile, solutions like digital workers alleviate the burden of repetitive tasks otherwise placed on staff. Finally, security policy and automated solutions reduce the potential for insider threats and credentialed attackers from impacting critical assets or accessing sensitive information.

Embrace Gamification

Humans are complex, and an entire field of cognitive psychology is dedicated to exploring how the learning and development process improves, such as when education becomes interactive or involves additional senses. Gamification is the reinterpretation of training into an interactive format focused on actively leveraging knowledge in real-time to solve complex problems, puzzles, or scenarios, rather than just memorizing concepts or reading from a slide presentation. The benefits of leveraging gamification in cybersecurity are three-fold.

1. Personnel, even those initially adverse to the gamification, exhibit improved understanding, internalization, and retention of critical information [23].
2. Scenario-based learning better teaches personnel to recognize threats and acclimates them to incident response practices.
3. Talent appreciates approaches to training that deviate from presentation formats without losing merit or complexity.

Automate with Digital Workers

Digital Workers, sometimes referred to as virtual employees, enhance and augment the workforce by combining AI, machine learning, RPA, and analytics to automate business functions from end to end. Leveraging digital workers may alleviate the burden that mundane and repetitive tasks place on the workforce, empower staff to allocate their time to mission objectives, and ensure that routine operations are consistently and accurately completed. Solutions are flexible and scalable, may be integrated with other solutions like the cloud, and can free resources for additional investment in talent acquisition or security solutions. Digital worker adoption should be tempered by the user's understanding of the technology, its potential impacts on associated AI and machine learning solutions such as the introduction of unintentional biases, and the tested assurance that the vendor solution will not facilitate adversarial compromise or empower insider threats.

Improve Insider Threat Deterrence, Recognition, and Reporting

In addition to recruiting, retaining, and educating talent, organizations also need to improve how they prevent their personnel from becoming malicious, negligent, or compromised insider threats. Based on a Ponemon Institute study of 6,803 insider-related incidents, Ponemon's *2022 Cost of Insider Threats Global* Report found that on average [24]:

- 56% involved negligence
- 26% involved a criminal insider
- 18% involved user credential theft

The 2021 Verizon Data Breach Investigations Report (DBIR) attributed ~22% of security incidents to malicious and unintentional insider threats. Meanwhile, a Stanford University study asserts that 88% of all data breaches are caused by an employee mistake. The 2022 Ponemon Cost of Insider Threats Global Report found that incidents involving malicious, negligent, and compromised users rose 44% over the past two years, with costs per incident up more than $15.38 million. Additionally, they found that:

- The cost of credential theft to organizations increased 65%, from $2.79 million in 2020 to $4.6 million in 2022.
- The time to contain an insider threat incident increased from 77 to 85 days, leading organizations to spend the most on containment.
- Incidents that took more than 90 days to contain cost organizations an average of $17.19 million annually.

Deterring insider threats is as much about "keeping honest people honest" as detecting the threat. Organizations can better deter and detect insider threats by increasing cyber-hygiene training and awareness, perhaps via gamification, leveraging digital workers to automate mentally frustrating tasks, or leveraging security solutions such as User-behavioral analytics to detect threats automatically. Cyber-hygiene training and awareness and a whole-of-organization approach to cybersecurity can also help mitigate the potential that an employee might inadvertently impose undue risks to an organization by providing data or knowledge that they don't realize could help adversaries foster attacks.

Similarly, more needs to be done to mitigate risk inherited from trusted partners or adopted solutions. For instance, organizations need to deploy behavioral analytics on the OT and IoT devices deployed within their environments to better understand any potential vulnerabilities that may provide access.

Adopt A Zero Trust Framework

Executive Order 14028 called on federal agencies to transition towards Zero Trust paradigms that reduce the impact and potential of threats by eliminating implicit trust and requiring continuous validation. Zero Trust assumes no network boundaries and requires all users to be authenticated, authorized, and continuously validated before permitting access to networks, data, or resources. In addition to identity management (User pillar) though, adopted frameworks should also apply the zero trust model to the Device, Network/Environment, Application, Data, Visibility, and Automation pillars.

Figure 1: DoD Zero Trust Reference Architeture Pillars

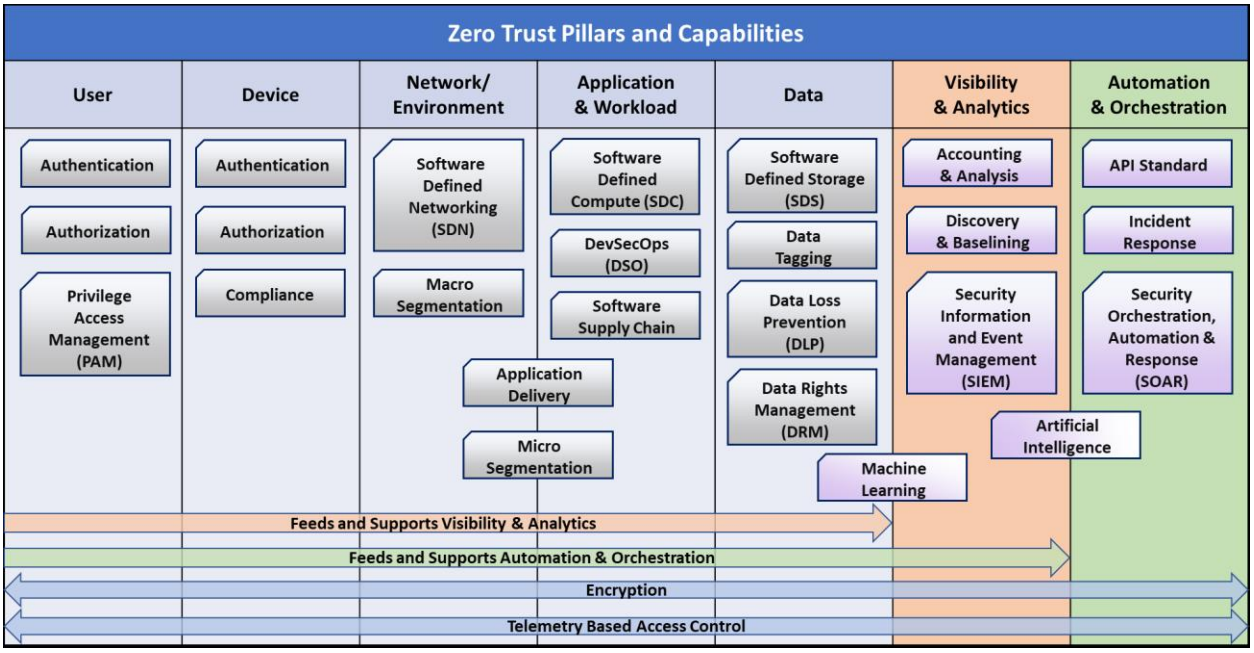

Figure 1 depicts the zero trust example pillars recommended by the Department of Defense.

The model limits how much an attacker can laterally move across the network, and it significantly reduces the impact a malicious insider could achieve [25]. Though public and private sector organizations have been slow to transition, Zero Trust is not a novel framework. Excellent resources, such as NIST 800-207, are readily available to help organizations implement zero trust [26].

Building Your Plan: How do We Get There from Here

At the ICIT 2022 Spring Briefing, facilitated in partnership with MFGS, inc. industry experts will share their experiences and perspectives on developing and implementing strategic plans that include automation, cloud migration, data lifecycle management, risk assessment, and an extensive selection of relevant topics. This publication will conclude with a high-level primer on some of the steps included in a holistic cybersecurity strategy. Cybersecurity strategies should be cyclical and adapt over time as necessary.

Evaluate Organizational Resources and Risk

A risk assessment must be conducted to identify and secure mission-critical networks, systems, and assets. The assessment combines threat intelligence, breach impacts, industry knowledge, and other essential metrics to determine the exposure of, estimate the risk to hardware, software, data, intellectual property, and resources, and determine the likelihood of an attack, how to best secure those assets against potential cyber threats, and what the potential impacts of incidents could cost an organization. In short, risk assessments are a vital but often underappreciated part of information security. No security strategy can be effective without an awareness of what is known and unknown. Moreover, no plan is effective unless assets are comprehensively secured according to their vulnerability, value, and potential for impact if compromised. David Wray expounds, “Both government

and industry need to evaluate organizational and resource risks. Core technology companies and platform vendors have the unique opportunity to change the technical landscape and hurt attacks from adversaries by building secure mature, secure software, technology, and documentation on how to configure to reduce risks."

Incorporate Knowledge About the Threat Landscape

Cyberwarfare is asymmetric against the defender. Proactive planning depends on aggregating as much relevant information as possible on vulnerabilities, active threat actors, and attacker trends and methodologies from industry stakeholders, public sector partners, academia, and sector thought leaders. After assessing the risk, threat intelligence is still useful to help inform long-term investments in security solutions. Further, information sharing helps improve security for all. The more collaboratively information is shared, the fewer attackers succeed in their campaigns, the lower the perceived profitability of cyberattacks in proportion to the necessary resource allocation. Eventually, the number of active cyber-attackers may decrease. David Wray, ICIT Fellow and Strategic Program Manager, MFGS, Inc., suggests, "Although CISA's new Joint Cyber Planning Office (JCPO) has the lead on knowledge sharing and collaboration, dedicated engineering and threat intelligence firms, core technology providers, and federal, civilian, and military intelligence agencies should be encouraged to participate in working groups." He adds, "The best offensive strategies start with understanding your established defenses."

Develop a Practical, Realistic, and Proactive Plan

Too many leaders chase vendor security promises or seek "silver bullet" solutions to cybersecurity. The only way to prevent compromise, mitigate threats, remediate vulnerabilities, and minimize impacts is to have a practical and realistic understanding of the threat landscape, the risk to mission-critical systems, and capabilities of the organization and to proactively adopt policies, procedures, and technologies to secure people, processes, systems, and data in the short and long term. Cybersecurity is an endless, cyclical marathon, not a short sprint. Long-term and sustainable security depends on setting achievable goals, measuring progress, continuously reevaluating posture and direction, adapting when necessary, and building momentum.

Communicate the Strategy and Evangelize Stakeholders

Any security strategy will fail if the priorities or tenets compete with those of leadership, key stakeholders, or those tasked with operating within the policies, procedures, or solutions adopted. A lack of funding, shadow IT, or countless other obstacles could inhibit effective security due to poor communication or articulation of security processes and goals. Instead of implementing solutions without consideration of how it might impact the performance of non-cybersecurity personnel, it almost always proves more effective in both the short and long term to have a discussion focused on why the solution was adopted, how it is implemented, what it does, how it improves efficiency, what benefits it brings to the organization, and what impacts or negative outcomes the organization could face if a solution is not adopted or if personnel do not adhere to an internal policy. Further, leaders, especially in the public sector, cannot wait on legislation or top-down guidance to force them to create change, improve cybersecurity, or implement meaningful policies. Waiting to implement proactive solutions and policies may hinder any potential or momentum for transformative change. NIST, OMB, GAO, and other agencies offer excellent guidance that can be leveraged to guide the proactive improvement of digital

defenses. Public sector cybersecurity leaders should set the examples for personnel internal and external to their organization to follow. David Wray recommends, “Leaders can request help and funding from OMB and the Whitehouse, establish communities of practice and create government-wide common tools and services.”

Foster Long-Term Maturity and Growth

Cybersecurity requires cooperation, collaboration, and communication across an organization for a prolonged period. It is a whole-of-organization effort guided by the information security team, usually under the direction of the CISO. Establishing and retaining consistent cybersecurity requires commitment, vigilance, agility, and proactivity. It requires stakeholders at all levels to recognize the value that cybersecurity brings as a business driver and then go far beyond minimalistic check box compliance models or low-resource strategies. Do you want your data or safety to depend on someone doing the bare minimum? Doing the bare minimum will lead to as disappointing results in cybersecurity as it would in any other aspect of life. You have to do much more than the minimum if you are “playing to win.” Mr. Wray opines, “Playing to win means having the ability to ruthlessly prioritize risks to minimize the impact of successful attacks, triage, and bring to bear rigorous cyber/compliance procedures. Resources will always be scarce, but organizations must be able to continuously evolve and deploy new capabilities to keep pace with the threat landscape.”

Adversaries are constantly innovating, collaborating, and evolving. As effective cybersecurity solutions or strategies popularize, adversaries shift to less resource-intensive attack models and targets like the software supply chain, vulnerable applications, and cloud/SaaS (Software as a Service) attack vectors. To not be the “lowest hanging fruit," “weakest link,” or “easiest target,” organizations must shift their culture, solution acquisition plan, talent strategy, and leadership mindset to proactively plan against the all-too-real threats against their networks, systems, people, data, and assets.

Conclusion

The impacts of events of the past year, ranging from increases in cybercrime to a transition to remote work and the cloud, were unforeseeable. Hindsight benefits our reflection, evaluation, and analysis, but we do not know what the future may yet hold. Cybersecurity is a mercurial field, and a strategic planning mindset is essential to preempt emerging threats and attacks. At the April 6, 2022, ICIT Spring Briefing, “Playing to Win: Using Strategy to Create Your Cybersecurity Battle Plan," facilitated in partnership with MFGS, inc. Cybersecurity thought leaders from across the public and private sectors will expand on some of the themes discussed in this publication and offer greater depth and insights through their experience in developing and implementing comprehensive and proactive cybersecurity strategies that ensure the security of individual organizations and our nation.

Sources

[1]"Software Supply Chain Attacks", *Dni.gov*, 2022. [Online]. Available: https://www.dni.gov/files/NCSC/documents/supplychain/Software_Supply_Chain_Attacks.pdf. [Accessed: 23- Mar- 2022].

[2]"Cost of a Data Breach Report 2021", *Ibm.com*, 2021. [Online]. Available: https://www.ibm.com/security/data-breach. [Accessed: 23- Mar- 2022].

[3]J. Williams, "What You Need To Know About the SolarWinds Supply-Chain Attack | SANS Institute", *Sans.org*, 2020. [Online]. Available: https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/. [Accessed: 23- Mar- 2022].

[4]"M-Trends 2021", *FireEye*, 2022. [Online]. Available: https://content.fireeye.com/m-trends/rpt-m-trends-2021. [Accessed: 23- Mar- 2022].

[5]"The 2021 Evil Internet Minute", *Riskiq.com*, 2021. [Online]. Available: https://www.riskiq.com/resources/infographic/evil-internet-minute-2021/. [Accessed: 23- Mar- 2022].

[6]"Vulnerability and Threat Trends Report 2021 Cybersecurity comes of age", *Skybox Security*, 2021. [Online]. Available: https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox-Security-vulnerability-and-threat-trends-report-2021.pdf. [Accessed: 23- Mar- 2022].

[7]"Internet Crime Report 2020", *Ic3.gov*, 2020. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf. [Accessed: 23- Mar- 2022].

[8]"Cybercrime Will Cost the World US$6 Trillion by the End of the Year: Study", *CISO MAG | Cyber Security Magazine*, 2022. [Online]. Available: https://cisomag.eccouncil.org/cybercrime-will-cost-the-world-us6-trillion-by-the-end-of-the-year-study/. [Accessed: 23- Mar- 2022].

[9]"Threat Landscape Trends – Q1 2020", *Symantec-enterprise-blogs.security.com*, 2020. [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-q1-2020. [Accessed: 23- Mar- 2022].

[10]"2021 Data Breach Investigations Report", *Verizon.com*, 2021. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/. [Accessed: 23- Mar- 2022].

[11]"NCSA & SBA Small Business Resources - Stay Safe Online", *Stay Safe Online*, 2022. [Online]. Available: https://staysafeonline.org/cybersecure-business/ncsa-sba-small-business-resources/. [Accessed: 23- Mar- 2022].

[12]"45% of fraud attacks worldwide abuse brand names - Atlas VPN", *Atlasvpn.com*, 2022. [Online]. Available: https://atlasvpn.com/blog/45-of-fraud-attacks-worldwide-abuse-brand-names. [Accessed: 23- Mar- 2022].

[13]"Check Point Research: Cyber Attacks Increased 50% Year over Year - Check Point Software", *Check Point Software*, 2022. [Online]. Available: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/. [Accessed: 23- Mar- 2022].

[14]R. Hummel and C. Hildebrand, "Crossing the 10 Million Mark: DDoS Attacks in 2020 | NETSCOUT", *NETSCOUT*, 2021. [Online]. Available: https://www.netscout.com/blog/asert/crossing-10-million-mark-ddos-attacks-2020. [Accessed: 23- Mar- 2022].

[15]"Open Source Code", *U.S. Department of Commerce*, 2022. [Online]. Available: https://www.commerce.gov/about/policies/source-code. [Accessed: 23- Mar- 2022].

[16]"Sonatype's 2021 State of the Software Supply Chain", *Sonatype.com*, 2021. [Online]. Available: https://www.sonatype.com/resources/state-of-the-software-supply-chain-2021. [Accessed: 23- Mar- 2022].

[17]"2021 State of Open-Source Security Report", *Contrastsecurity.com*, 2021. [Online]. Available: https://www.contrastsecurity.com/the-state-of-the-oss-report-2021. [Accessed: 23- Mar- 2022].

[18]F. Zandt, "Ransomware attacks are on the rise. These are the industries most a risk", *World Economic Forum*, 2021. [Online]. Available: https://www.weforum.org/agenda/2021/11/industries-affected-ransomware-cybersecurity-cybercrime/. [Accessed: 23- Mar- 2022].

[19]"22 Shocking Ransomware Statistics for Cybersecurity in 2021", *Safeatlast.co*, 2021. [Online]. Available: https://safeatlast.co/blog/ransomware-statistics/. [Accessed: 23- Mar- 2022].

[20]R. Davidson, "Malware-as-a-service is the growing threat every security team must confront today", *Securitymagazine.com*, 2021. [Online]. Available: https://www.securitymagazine.com/articles/96024-malware-as-a-service-is-the-growing-threat-every-security-team-must-confront-today. [Accessed: 23- Mar- 2022].

[21]"The (ISC)² Cybersecurity Workforce Study", *(ISC)2*, 2021. [Online]. Available: https://www.isc2.org/Research/Workforce-Study. [Accessed: 23- Mar- 2022].

[22]"Cybersecurity Supply And Demand Heat Map", *Cyberseek.org*, 2022. [Online]. Available: https://www.cyberseek.org/heatmap.html. [Accessed: 23- Mar- 2022].

[23]B. Wolfenden, "Gamification as a winning cyber security strategy", *Computer Fraud & Security*, vol. 2019, no. 5, pp. 9-12, 2019. Available: 10.1016/s1361-3723(19)30052-1.

[24]"2022 Ponemon Cost of Insider Threats Global Report | Proofpoint US", *Proofpoint*, 2022. [Online]. Available: https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats. [Accessed: 23- Mar- 2022].

[25]"Department of Defense (DOD) Zero Trust Reference Architecture", *Department of Defense*, 2021. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf. [Accessed: 23- Mar- 2022].

[26]S. Rose, O. Borchert, S. Mitchell and S. Connelly, "NIST SP 800-207 Zero Trust Architecture", *Csrc.nist.gov*, 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-207/final. [Accessed: 23- Mar- 2022].