Culture Comes First in Any Successful Cybersecurity Plan

Months into the new decade of 2020 and the wounds of some 2019 cybercrimes on public and private sector organizations have yet to heal.

In early January, New Orleans officials shared that efforts to scan computers for ransomware were still underway three weeks after an attack on the city.[1] Another six to eight months were estimated for operations to return to normal, while the financial impact stood at more than seven million dollars to date.[2] June came, and 20% of the city's operations had yet to return to normal,[3] demonstrating the lasting effects when one or more employees are lured by a phishing email.[4]

Japan-based manufacturer Mitsubishi Electric disclosed details of a data breach that had begun months earlier in 2019 — the result of a new vulnerability in its anti-virus software for which a patch had not yet been released. Two-hundred megabytes of files were stolen and the data of 8,000+ employees, 40 servers and 120 computers compromised. Clients such as the Nuclear Regulatory Commission may have also been impacted.[5] As of May, the impacts were still being felt, with Japan investigating the company for potential loss of sensitive data related to missile prototypes.[6]

[1] Williams, J. (2020, January 2). *Cyberattack update: New Orleans police, court systems to be restored by Monday, officials say.* NOLA. https://www.nola.com/news/article_d880d35a-2d9b-11ea-aabe-ff584b1dca3e.html

[2] Curth, K. (2020, January 15). *City of New Orleans says it will take months to recover from recent cyber attack.* FOX 8. https://www.fox8live.com/2020/01/15/city-new-orleans-says-it-will-take-months-recover-recent-cyber-attack/

[3] Lux, T. (2020, June 16). *New Orleans is 80 percent recovered from last year's cyberattack, officials say.* New Orleans Public Radio. https://www.wwno.org/post/new-orleans-80-percent-recovered-last-year-s-cyberattack-officials-say

[4] Wray, S. (2019, December 23). *New Orleans cyber attack 'triggered by phishing email'.* SmartCitiesWorld. https://www.smartcitiesworld.net/news/news/new-orleans-cyber-attack-triggered-by-phishing-email-4884

[5] Ikeda, S. (2020, February 5). *Data breach at Mitsubishi Electric caused by zero-day vulnerability in antivirus software.* CPO Magazine. https://www.cpomagazine.com/cyber-security/data-breach-at-mitsubishi-electric-caused-by-zero-day-vulnerability-in-antivirus-software/

[6] Lyngaas, S. (2020, May 20). *Japan investigates Mitsubishi Electric breach and national security concerns.* CyberScoop. https://www.cyberscoop.com/mitsubishi-japan-missile-data-breach/

Meanwhile, new crimes have continued making headlines, such as one in South Carolina, where a local utility fell victim to a cyberattack. Greenville Water, which serves almost 500,000 customers, experienced a network outage, also due to a phishing email. Phone and online payment systems went offline for nearly a week.[7] Customer data was reportedly unaffected, but operations were hampered, as personnel were forced to rely on manual means of doing business.

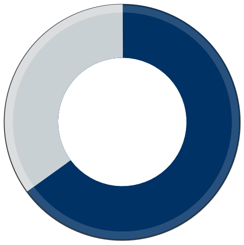
Levy County Sheriff's Office in Florida also lost use of phone lines when a denial-of-service attack ended in a demand for ransom. Though only the non-emergency phone lines were affected, 9-1-1 call takers were left to field those non-emergency calls in addition to those from residents needing help.[8] The county attempted to resolve the issue by moving the non-emergency lines to a new system, but the attack resumed on those lines.[9]

These examples reveal many truths about cybercrimes. No sector is safe as hackers continue to discover new ways to infiltrate systems and refine existing schemes to disrupt operations, whether to collect ransom or to simply satisfy a wicked desire. This makes organizations of all types and sizes vulnerable. The effects can be long-lasting and far-reaching, even spanning international borders. Beyond the monetary price tag, cybercrimes can damage an organization's brand — its public perception or shareholder value — and in some sectors, result in the loss of lives. With so much at stake, the time is now for all organizations to put in place cybersecurity measures or to examine existing plans.

[7] Coble, S. (2020, January 29). Cyber-attack on US water company causes network outage. *Infosecurity Magazine.* https://www.infosecurity-magazine.com/news/cyber-attack-on-greenvillewater/

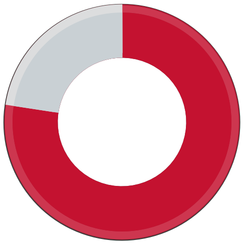
[8] Harrar, L. (2020, July 17). *Levy County Sheriff Office's non-emergency phone lines held for ransom.* WCJB. https://www.wcjb.com/2020/07/17/levy-county-sheriff-offices-non-emergency-phone-lines-held-for-ransom/

[9] WCJB. (2020, August 7). *Non-emergency phone lines down at Levy County Sheriff's Office.* https://www.wcjb.com/2020/08/08/non-emergency-phone-lines-down-at-levy-county-sheriffs-office/



65%

of global organizations report cyberattacks are growing more severe



77%

have still yet to implement a consistent cybersecurity response

Today's Cybersecurity Landscape

A 2019 global study, sponsored by IBM Security and conducted by the Ponemon Institute, found 77% of respondents have yet to implement a cybersecurity response plan consistently across their organizations.[10] This is despite 65% experiencing an increase in the severity of attacks. More than half name the leak of valuable information (56%) and decreased employee productivity (51%) as their biggest indicators of increased severity, both impacting operations and the bottom line. A 2019 Accenture Security study on the cost of cybercrime reports the combined damage of these two issues alone stands at close to $10 million — four million due to business disruption and almost six million for loss of information — per organization.[11] And it's likely the financial damage will continue to increase, since the costs of dealing with cybercrimes have risen 72% over the past five years.

The latter study also reveals another trend in cybercrime — the move to people-driven cyberattacks. No longer are hackers relying on systems to install malware and commit other wrongdoings. Today, they're targeting the people within your organization. They're counting on them to interact with phishing emails, clicking links and opening files, to launch their attacks.[12] As technology advances to make it easier for bad actors to disguise their efforts, organizations without cybersecurity measures in place are sure to suffer.

To secure operations from attacks, cybersecurity must not only be in practice by network and security personnel, it must also be ingrained within organizational culture — a commitment shared by every person within an organization, from the top down. This shared responsibility must be maintained through coordination, cooperation and collaboration, with solid communication at the core, to ensure the best possible outcome in any situation.

[10] IBM Security. (2019, April 11). *IBM study: More than half of organizations with cybersecurity incident response plans fail to test them.* https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them

[11] Accenture. (2019). Ninth annual cost of cybercrime study. [Infographic]. https://www.accenture.com/_acnmedia/PDF-99/Accenture-Cost-Cyber-Crime-Infographic.pdf#zoom=50

[12] More than 99 percent of cyberattacks need humans to click. (2019, September 13). *Security.* Retrieved June 20, 2020, from https://www.securitymagazine.com/articles/90908-more-than-99-percent-of-cyberattacks-need-humans-to-click

The Critical Role of Communication in Cybersecurity

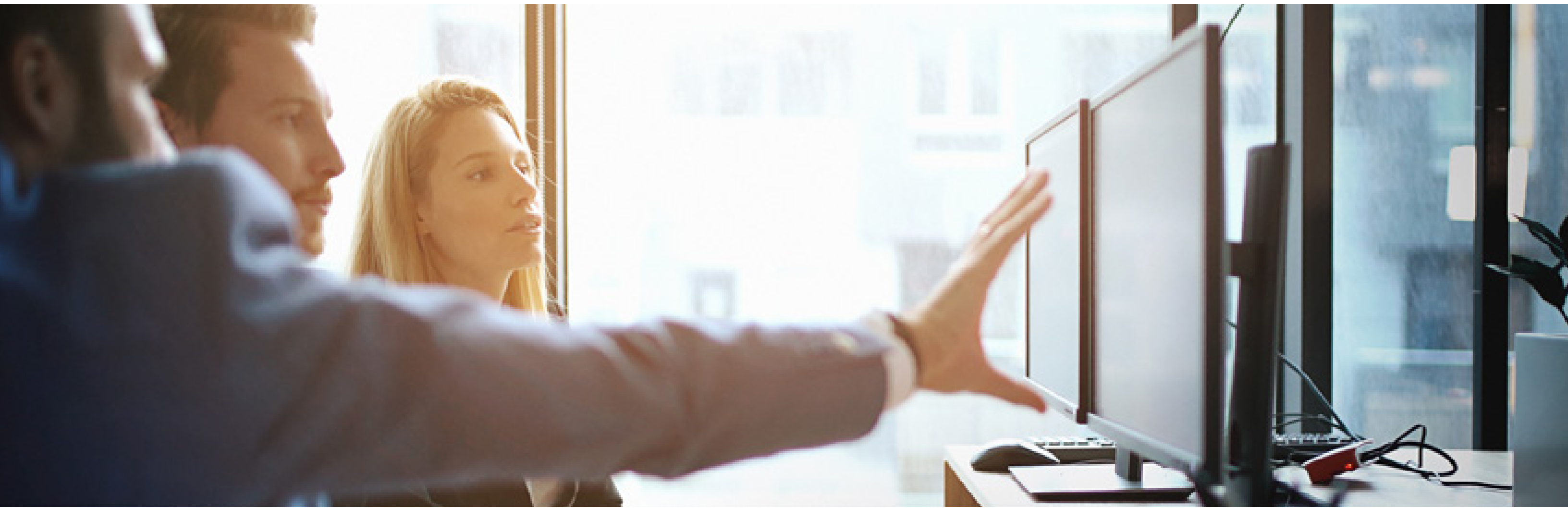
The role of communication as it relates to cybersecurity is both vital and multi-faceted. The Ponemon Institute study found that regular communication is an indicator of cybersecurity success. “High performers” — those organizations most confident in their security posture — communicate with senior staff on cybersecurity matters more frequently than “average performers.” It’s believed senior management has a better understanding of how cyber resilience relates to their organization’s reputation because of ongoing communication, which helps secure funding for cybersecurity needs.

Some may consider effective communication most critical during and following a cybercrime, when response and recovery efforts are underway. It’s then you engage stakeholders at various levels, whether a board of directors, staff, concerned citizens or others, to put plans in motion or provide status updates. Yet, when you consider the work that takes place in mitigating and preparing for cyberattacks, the role of communication is equally important. These are the times to make cybersecurity plans and their revisions part of your organizational culture.

In preparation, communication drives awareness of cybersecurity measures and their importance, as well as to inform personnel of what’s expected of them to enable the organization to become cyber resilient. Following a cyberattack, it’s important to communicate with management on areas lacking adherence so that they can then communicate with their teams and help mitigate the impact of future crimes. Opening up the lines of communication within your organization may also identify other risk factors, allowing you to refine your cybersecurity plan and make the most effective use of best practices for its implementation and maintenance.

Cybersecurity Best Practices

The nature of cybersecurity can lead some to believe a strong cybersecurity program is built on technology. But people and processes are just as important. That's why a well-rounded program will not only consider physical assets, but also the human actions and the processes behind them.



Best Practices for People in Cybersecurity

Consider the following best practices for how to most effectively engage people in cybersecurity planning and execution.

Get Upper-Level Buy-In

As noted, organizations benefit from communicating cybersecurity efforts with senior management. Still, this doesn't ensure cybersecurity is part of organizational culture. A *Harvard Business Review* article cites the "back office" treatment of designated cybersecurity roles, viewed as support to the overall organization rather than an integral component for success. This dampens the influence of these individuals to make the necessary impact across the organization.[13] For these reasons, the buy-in and participation of senior management is critical to selling its importance.

To open the door, it's important to speak in terms these leaders can identify with. This means explaining how cybersecurity measures align with the organization's goals. Make your case in non-technical language and with a positive outlook, offering solutions to problems — and demonstrate with numbers when possible. When you show the measurable value of such a program, they'll be more likely to use their influence in the boardroom and throughout the organization in support.

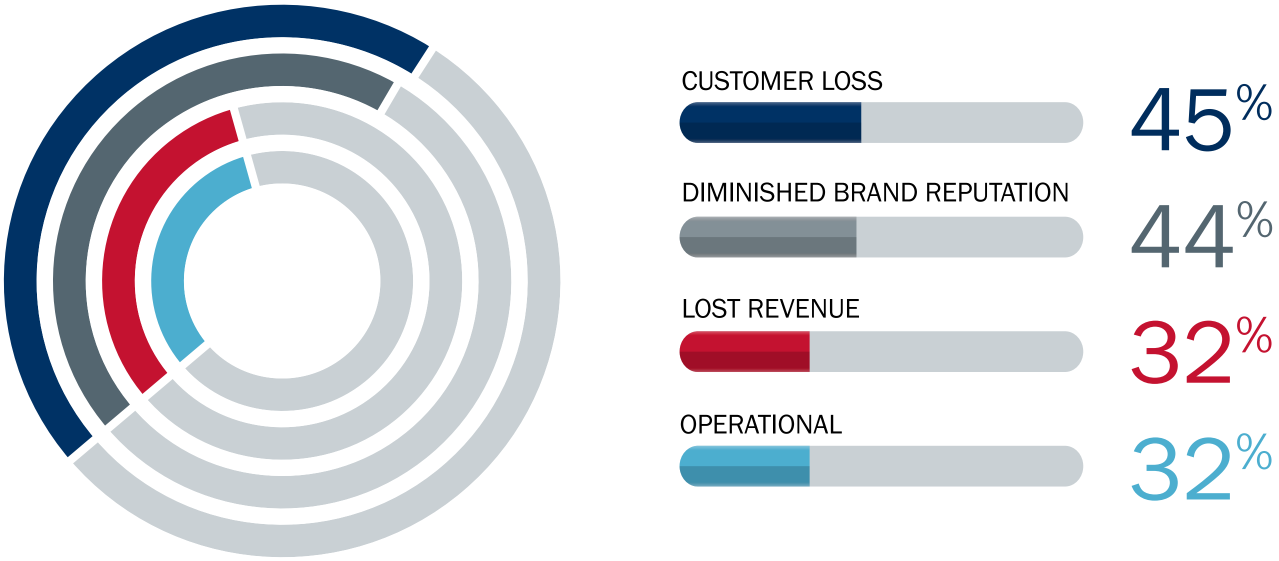
[13] Doan, M. (2019, November 27). Companies need to rethink what cybersecurity leadership is. *Harvard Business Review.* https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is

Assemble a Cross-Functional Team

Consider the biggest impacts of a cyberattack as reported by executives: customer loss (45%), diminished brand reputation (44%), lost revenue (32%) and operational (32%).[14] While in the public sector, agencies and organizations face negative public perception and exorbitant expenses due to impaired operations and recovery efforts. While all these damages, no matter the sector, stem from technology, they're not issues a Chief Information Security Officer or Chief Technology Officer can repair. Instead, managers and other staff resources, from such departments as legal, human resources, sales and marketing, as examples, will be called on for response. Likewise, they should also be involved in establishing and maintaining the cybersecurity program.

When an event occurs, these stakeholders will need to understand how they'll be contacted and what steps they must take to respond and recover. They'll also be vital in efforts to make cybersecurity part of organizational culture, as they lead their departments in recommended practices and help to secure their sensitive data and other assets. Plan to meet on a regular basis to know the overall cybersecurity posture, discuss changes within the organization, and uncover new risks or update practices. By doing so, you will be proactively maintaining and strengthening your program.

4 Biggest Impacts of a Cyberattack



[14] Radware. (2019, June 18). *Radware survey: Cybersecurity is no longer a cost factor for $1B organizations, rather it's a business driver.* https://blog.radware.com/campaign/2019/06/c-suite-perspectives-2019/

Form an Incident Response Team

When a cyberattack occurs, you'll need a team of people trained and ready to execute critical activities and mitigate the impact. The Council for Registered Ethical Security Testers (CREST) explains that this team — your incident response team — may be made up of your own staff or may be outsourced to a service provider.[15] In many cases, it will be a combination of both. Regardless, CREST recommends your team should be supported by various stakeholders within your organization, such as from HR, legal and public relations — likely those who make up your cross-functional team.

The incident response team should:

- Be empowered to seize equipment and monitor questionable activity
- Manage information sharing, knowing established communications plans (who, what, when and how)
- Have a firm understanding of cybersecurity plans and the process for escalation
- Know what's required for reporting on the various types of cyberevents

CREST also provides suggested tools for your incident response toolkit to help ensure readiness and speed response efforts.

[15] CREST. (2014). *Cyber security incident response guide.* (Version 1). https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

Best Practices for Processes in Cybersecurity

With the right people in place for planning and action, it is time to ensure the same for policies and processes. The following best practices relate to some of the most critical elements for building and maintaining your cybersecurity program. As you work through them, document every detail for consistency among your team members on the front lines as well as behind the scenes.

Develop a Cybersecurity Policy

All cybersecurity stakeholders have the responsibility of developing the cybersecurity policy — or the standards everyone with access to your organization's assets must follow — for maintaining a strong cybersecurity posture. The Infosec Institute breaks such a policy into three categories:[16]

1. **Physical security** — the means of protecting physical assets, such as doors, surveillance and alarms
2. **Personnel management** — the guidelines for employee conduct as it relates to cybersecurity (e.g., password management)
3. **Hardware and software** — the technology and network controls system and network administrators must use

Once the policy is written, Infosec encourages periodic security audits to know if your policy is working and to determine exposure to threats. They also stress the importance of enforcing this policy across your audience, which includes the people within your organization as well as anyone external who uses its assets.

[16] Infosec. (n.d.). *An introduction to cyber security policy.* https://resources.infosecinstitute.com/cyber-security-policy-part-1/#gref

Establish a Regular Training Program

While it's critical that your cross-functional and incident response teams complete ongoing training and, for some, achieve certifications, there's a bigger need within your organization — your general workforce. A Kaspersky Lab survey found that only 12% of employees understand their organization's IT security policies and rules.[17] With hackers targeting people, this leaves the majority unaware of how to defend themselves and your organization. That's why Infosec names awareness and education a vital step following development of your cybersecurity policy.

To start, the Center for Internet Security® (CIS) recommends stakeholders conduct a skills gap analysis to uncover the areas in which employees need education.[18] This will help you to build a baseline training program. CIS recommends instruction on how to identify phishing emails and phone scams. Other areas may include policies for password security and use of email and the internet.

Have a Plan of Action and Milestones

Launching a cybersecurity program can be daunting. And while its necessity may require fast action, your team's moves should not be made in haste and leave room for error. A Plan of Action and Milestones (POAM) can help you move ahead strategically and stay focused.

While the POAM can help you detail tasks, including necessary resources, milestones and completion dates for getting your program off the ground, the National Institute of Standards and Technology (NIST) names the POAM a requirement in tracking remedial actions and updating your system security plan following a security certification.[19] NIST's cybersecurity framework was developed with critical infrastructure organizations in mind, but has become the standard for global organizations of all types. Seek out guidance and resources from NIST and other cybersecurity experts to develop your program. For example, the Federal Risk and Authorization Management Program (FedRAMP) offers a POAM template on its website that can be modified for your use.[20]

[17] Rayome, A. D. (2018, January 11). *88% of employees have no clue about their organization's IT security policies.* TechRepublic. https://www.techrepublic.com/article/88-of-employees-have-no-clue-about-their-organizations-it-security-policies/

[18] Center for Internet Security. (n.d.). *Implement a security awareness and training program.* https://www.cisecurity.org/controls/implement-a-security-awareness-and-training-program/

[19] Swanson, M., Hash, J., & Bowen, P. (2006). *Guide for developing security plans for Federal information systems.* NIST.gov. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf

[20] FedRAMP. (n.d.). *Developing a plan of actions & milestones (POA&M).* https://www.fedramp.gov/developing-a-plan-of-actions-milestones/

Best Practices for Technology in Cybersecurity

The role of technology is paramount in maintaining your cybersecurity posture, and depending on your organization, can be broad and multi-faceted. Your industry and business drivers, as well as your organization's risks and systems, are some variants that make your cybersecurity program unique. Yet, there are still best practices all organizations should apply as it relates to technology.

Get Serious About Patch Management

The 2020 CISO Benchmark Study from Cisco® found almost half of its respondents were victims of a security incident due to an unpatched vulnerability.[21] And 68% of them lost at least 10,000 data records. Conversely, attacks that stemmed from other causes impacted fewer organizations at this scale. Only 41% lost 10,000 or more records over the same time period. This demonstrates hackers' commitment to seeking out those with vulnerabilities, as well as the need for a strong patch management program.

A first step to such a program is to make an inventory of all systems and prioritize them based on their level of risk. Stay in touch with your solution providers to know when an update is necessary. Though you should apply the patch as soon as possible, be sure to test it prior to doing so. Should you not have the time and resources to commit to patch management best practices, outsource the critical responsibility to solution providers with dedicated resources for these and other maintenance tasks when possible. Leverage their expertise while focusing on other cybersecurity initiatives.

[21] Cisco. (2020). *Securing what's now and what's next.* https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-ciso-benchmark-cybersecurity-series-feb-2020.pdf

Implement Intrusion Prevention and Detection Systems

CIS names boundary defense one of its foundational controls for maintaining information security. To monitor and manage network traffic and protect hackers' entry, it recommends a multi-layered defense approach that includes network-based intrusion detection systems (IDS) and intrusion prevention systems (IPS).[22]

The role of an IDS is to monitor network traffic, comparing information packets to those in the IDS database to identify malicious behaviors. The IPS works to deny malicious traffic and prevent breach. Other elements of robust IDS and IPS include well-defined firewalls, port scanning, system logs, as well as alerts, mobilizing a dedicated security team into action when necessary.

Use Multi-Factor Authentication

COVID-19 prompted the need for rapid mobilization of remote employees across all industries, public and private. The pandemic left many organizations unprepared and vulnerable, despite the majority — 72% percent per a survey by Cybersecurity Insiders and Pulse Secure — having plans to implement a zero trust model in 2020.[23] This type of security framework prevents organizations from automatically trusting anyone or anything, no matter if inside or outside the network perimeter. Verification is required, and multi-factor authorization (MFA) is a clear way to obtain it.

MFA requires employees to provide two or more credentials at login for a user-friendly, yet strong layer of additional security. A flexible authentication policy allows you to adapt required authentication to your level of risk, such as being more strict for remote employees than those in your facility.[24] MFA and other means of security and access management enhance your ability to stay safe in any situation.

[22] Center for Inter¬¬net Security. (n.d.). *CIS Control 12: Boundary Defense.* https://www.cisecurity.org/controls/boundary-defense/.

[23] Pulse Secure. (2020). *2020 Zero Trust Progress Report.* https://www.pulsesecure.net/resource/2020zero-trust-report/

[24] Litton, J. (2020, April 29). Council post: Businesses need to adopt a zero-trust approach to stay secure while working remotely. *Forbes.* https://www.forbes.com/sites/forbestechcouncil/2020/04/29/businesses-need-to-adopt-a-zero-trust-approach-to-stay-secure-while-working-remotely/

A Look at Security and Access Management

Access management is vital for cybersecurity on several levels. While it begins within your walls and extends to employees everywhere, standards must also exist for the third-party providers you rely on to provide critical systems and services. A 2018 survey by the Ponemon Institute found that 56% of organizations were victims of a breach caused by a third-party vendor.[25] The CIA triad, which represents three pillars — confidentiality, integrity and availability — is a widely-adopted security model that works to maintain data integrity and ultimately, operational integrity.

Knowing the importance of communications for maintaining your cybersecurity posture and responding to and recovery from incidents, let's examine necessities for mission-critical communications systems and their providers under the CIA triad.

1

PILLAR ONE

Confidentiality

Access to information by unauthorized individuals is prohibited.

2

PILLAR TWO

Integrity

Information remains intact and without unauthorized modification.

3

PILLAR THREE

Availability

Authorized individuals have access to the information they need, right when they need it.

[25] Korolov, M. (2019, January 25). *What is a supply chain attack? Why you should be wary of third-party providers.* CSO. https://www.csoonline.com/article/3191947/what-is-a-supply-chain-attack-why-you-should-be-wary-of-third-party-providers.html

1

PILLAR ONE

Confidentiality

You expect your mission-critical communications system to have controls in place that protect your data, whether local to the system or transported across your network. But, know these are only as strong as the controls and policies your technology providers have in place. Their measures for confidentiality can be assigned to two categories — Authentication and Authorization.[26] The necessary controls include:

- **Identity assurance** — assignment of access permissions to authorized individuals by means of unique user credentials, secure Windows® Active Directory® and central distributor user management.
- **System data encryption** — prevention of unauthorized penetration of critical systems via secure access and data transport, including end-to-end password encryption, external interface encryption using the Advanced Encryption Standard, and key management.
- **Secure data exchange** — use of secure transfer protocols for data exchanges between your organizations; these may include secure remote access to your network, patch management via Secure File Transfer Protocol, and controlled login credentials with link expiration.
- **Secure intra-system communication** — use of secure protocols to strengthen against packet sniffing and other attempts by hackers; protocols may include Secure Shell (SSH)/ Secure File Transfer Protocol (SFTP) or Hypertext Transfer Protocol Secure (HTTPS)/ Transport Layer Security (TLS).
- **Logical control** — authentication and identification policies that restrict unauthorized access, including stringent password policies, role-based access and network segregation/ isolation where required.
- **Physical access control** — the prevention of unauthorized access to secure facilities and critical equipment; means may include two-factor authentication, visitor logging systems, video surveillance and locked equipment cabinets.

[26] Fruhlinger, J. (2020, February 10). *The CIA triad: Definition, components and examples.* CSO. https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html

2

PILLAR TWO

Integrity

Confidentiality measures serve to help ensure data and system integrity. But, the NIST has warned not to overlook this critical CIA pillar, reinforcing its importance to maintain both confidentiality and availability.[27] This requires your communications system providers ensure no unauthorized access or alteration of communications and data at all levels — devices, their hardware, software and data, as well as the network. Safeguards to ask technology vendors about include:

- **Source code control management** — adoption of version control to ensure software integrity — quality, consistency and security — throughout development and delivery; complete management includes source code analysis, regression testing and quality control validation.
- **Change management** — restriction of system access and assignment of logical access controls, as well as adoption of change auditing, to mitigate unauthorized alteration and to enable the forensic reconstruction of events.
- **Hashing algorithm** — calculation of a data set before its transit and again at its destination using a hash function such as SHA-2; comparison of both calculations ensure data integrity between the source and its endpoint.
- **Data assurance** — validation of software deployments and revisions to ensure components maintain compatibility and latest code build; agile methodologies are used and include data normalization.
- **Malware management** — commitment to a flexible malware policy that meets your needs and standards, provides streamlined deployment and simplifies management, including support of antivirus policies and directories' whitelist baselines.
- **Device access control** — removing or disabling of unrequired or unused services or ports, including USB and RJ-45 ports, to reduce unauthorized access, modification or harmful code introduction to system components.

[27] Irwin, L. (2018, April 5). *How NIST can protect the CIA triad, including the often overlooked 'I' – integrity.* IT Governance. https://www.itgovernanceusa.com/blog/how-nist-can-protect-the-cia-triad-including-the-often-overlooked-i-integrity

3

PILLAR THREE

Availability

Denial-of-service (DoS) attacks are on the rise. By 2023, Cisco estimates the number of distributed denial-of-service (DDoS) attacks will almost double, to 15.4 million. This is from 7.9 million in 2018.[28] The costs of such an attack are hefty, ranging from $120,000 to two million, depending on your organization's size.[29] And a DoS attack is only one threat to communications, which when unavailable, impacts operations and may even put lives at risk. This makes it critical to maintain and protect your communications system, devices, network and data to ensure availability. When evaluating technology providers, make sure they employ such measures as:

- **Survivability** — use of a distributed network and redundant components to eliminate single points of failure, enable access flexibility and improve system performance; measures should also include automatic failover, alarm notification by Simple Network Management Protocol (SNMP), geodiversity, and dynamic Session Initiation Protocol (SIP) routing.
- **Protection from threat agents** — implementation of procedures that protect against internal and external threats and help identify, minimize and eliminate exploitation of vulnerabilities; efforts should include security awareness training, vulnerability scanning and patch management.
- **Parallel processing** — use of multiple devices to diversify and simultaneously process tasks associated with interfaces, applications and services, improving scalability and performance; this should include load prioritization and balancing as well as Data Management System clustering.
- **System backup and restore** — restoration of system and data files and flexible revision management to meet your organization's changing needs; this includes rollback to the prior release and support of multiple, simultaneous revisions.
- **Platform support** — use of standard operating hardware and software environments to simplify development, deployment, maintenance and security; these include Microsoft® Windows Server®, VMware®, VxWorks®, commercial off-the-shelf personal computers and servers, and/or Cisco network compatibility.
- **Quality assurance (QA) testing** — end-to-end software validation to identify and resolve defects for product resilience; measures should include installation and upgrade testing, functional testing, failover and recovery testing, load and stress testing, and regression testing.
- **Business continuity plan** — proof of plans to ensure vendors' operational continuity to help ensure yours; these should outline procedures to maintain source code survivability and accessibility, including off-site source code backup, redundant development and QA platforms.

[28] Cisco. (2020, March 9). *Cisco Annual Internet Report (2018–2023) White Paper.* https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[29] Bulletproof. (2019). *Bulletproof Annual Cyber Security Report.* https://www.bulletproof.co.uk/industry-reports/2019.pdf

Moving Forward with Cybersecurity

There are many moving parts and pieces to a robust cybersecurity program. And without undivided attention to each, your organization is left exposed to a multitude of threats. This is why your cybersecurity program is bigger than a handful of people. It takes the efforts of everyone in your organization and some outside, too — particularly, your third-party providers. Knowing all that these vendors must bring to the table to protect their operations and yours, it is important to exercise due diligence in their selection, especially those providing communications systems.

The Federal Communications Commission once named communications systems "the backbone for information exchange," deeming such systems critical to national security and emergency preparedness.[30] They are not only vital for day-to-day operations, but also for responding to and recovering from malicious attacks. It is also their necessity that increasingly makes them a target.

This means you must employ standards, processes and technology that protect your mission-critical communications systems, and require your technology providers to do the same. It is also important that all parties test these plans to ensure their success. The IBM Security and Ponemon Institute study found that 54% of organizations do not perform these regular tests, which it says diminishes their ability to manage response efforts during a cyberattack.

Other ways to verify program effectiveness include seeking system certification and hiring of a third-party auditor. These initiatives can uncover weaknesses and strengthen your cybersecurity posture. More importantly, such a comprehensive strategy helps ensure your operational integrity, while minimizing negative impacts to your finances and reputation, among other potential and devastating risks.

Yet, to make this a reality, cybersecurity must be ingrained in culture, keeping its measures top of mind and ensuring readiness at all times. Start at the top and then work your way out to get everyone involved and to build a cybersecurity strategy that not only works for today but also prepares your organization for tomorrow.

[30] Federal Communications Commission. (n.d.). *Critical Infrastructure and Communications Security.* https://www.fcc.gov/general/critical-infrastructure-and-communications-security.