CYBERSECURITY RESILIENCE GUIDE

As a business owner or someone entrusted with protecting your organization's technology resources and data, you're already painfully aware of the need to defend against cyberattacks. Every day there is news of another entity falling prey to ransomware or massive data theft. The fallout can often be so severe that recovery is deemed to be impossible, and owners elect to cease operations. These events have become so frequent that many of us have become desensitized to them. But could it really be that the survival of your business is simply fated to a metaphorical roll of the dice? The answer, of course, is a resounding no. To be sure, cyberattacks themselves will never stop, but with the right approach to cybersecurity resilience, defending against them may not be as hard as it seems.

Every year Verizon publishes its Data Breach Investigations Report (DBIR). This is an interesting barometer of the cyberthreat landscape as it relates to data breaches. Taken as a whole, it's a useful guide that can help organizations in a variety of verticals understand the types of cyberthreats they're up against. The 2019 DBIR, for example, highlights a recent uptick in web application attacks, privilege misuse, and social engineering against targets in the financial and insurance sector. The report provides a lot of statistical information about recent breaches and the methods used to conduct them. Such information is key to effectively formulating your organization's strategy for cybersecurity, but there's more to the equation.

> Could it really be that the survival of your business is simply fated to a metaphorical roll of the dice?

This is where a lot of organizations struggle. We have all kinds of data about cyberthreats, but how do we know exactly what to do in order to protect ourselves? Complicating matters is the seemingly infinite number of vendors with security technologies that purport to be the magic bullet for all of our cybersecurity woes. We're led to believe that an impressive array of blinking lights is somehow the secret to effective protection against cyberthreats. Further, many business owners and managers defer all matters of cybersecurity to the IT department, which magnifies this product-centric, siloed approach and leads to significant gaps in protection. If risk management is not owned from the top down, security measures taken by IT can be ineffective. (See more in the Govern Your Environment section).

If you can have one takeaway from this guide, it should be that cybersecurity is not an IT problem, it's a business problem for which there may be an IT solution. Business owners and managers—with

Cybersecurity is not an IT problem, it's a business problem for which there may be an IT solution.

input and guidance from their IT resources—need to define, agree on, and endorse a strategy for cybersecurity from the top down, and this strategy needs to be rooted in a cybersecurity framework such as the NIST Cybersecurity Framework or the CIS Critical Controls. This guide is organized to align with the latter, but both NIST and CIS provide a wealth of practical and actionable guidance for organizations to formulate effective cybersecurity strategy in a threat-focused, vendor-neutral way.

Remember that cybersecurity is a never-ending process of continuous improvement, not a destination at which your organization can suddenly arrive. There's no magic cybersecurity bullet - defense in depth is the only viable strategy for surviving in today's threat landscape. Implementing the recommendations in this guide will not protect against every threat but will prevent your organization from being low-hanging fruit in the eyes of cybercriminals. Given the choice between an unprotected target and one that is well protected, attackers will go after the former nearly every time.

KEY ASPECTS OF CYBER RESILIENCE

- Govern Your Environment
- Know Your Systems
- Know Your Software
- Manage Your Vulnerabilities
- Restrict Administrative Privileges
- Harden System Configurations
- Monitor Your Logs
- Protect Email and Web Browsing
- Defend Against Malware
- Limit Accessible Services
- Be Able to Recover
- Protect the Boundary
- Protect Your Data
- Control Wireless Access
- Monitor and Control Accounts
- Security Awareness Training and Testing
- Respond to Incidents
- Penetration Testing

GOVERN YOUR ENVIRONMENT

Often times organizations are so keen to implement technical security controls like firewalls, intrusion prevention systems, and anti-malware software that they forego the processes of governance entirely. This is like putting the cart before the horse. Every organization has assets to protect—things like employees, information systems, and customer data. But without first understanding the specific assets that need to be protected—and the threats they need to be protected from—the implementation of any security technology is a shot in the dark. *In other words, how can we know whether it's the right tool for the job, and whether it's configured to do what it really needs to do?*

This is where a technology risk assessment is helpful. During this process, a qualified assessor evaluates an organization's information systems and technology infrastructure, determines the ways in which those assets are vulnerable, and then determines which threats are likely to exploit those vulnerabilities and cause risk. From there, the assessor can make specific recommendations to guide the organization in selecting mitigating security controls—whether they be technical, administrative, or procedural—in order to address the identified risk. This activity is a great way to lay the groundwork for developing an organization's cybersecurity strategy in an objective, ordered fashion.

The output of the technology risk assessment can also be used to guide the development of information security policies. Think of these as high-level statements from an organization's management about the way that certain functions (e.g., acceptable use of computers) shall be performed. Each policy can reference supporting procedures, standards, guidelines, or baselines to provide additional detail about the corresponding function. For example, an Acceptable Use Policy might state that employees are prohibited from using peer-to-peer file sharing applications or websites, and then the corresponding Acceptable Use Standard might specify which tools and configurations the IT department shall use in order to enforce this policy. As every organization is different, there's no authoritative list of mandatory policies. That said, many organizations have found it helpful to mirror their policy structures to risk-management frameworks like FISMA, ISO 27001/2, or COBIT. These cover the control objectives that are relevant to most organizations, and as such can provide an organized, comprehensive reference for policy development.

Many organizations are now purchasing cyber liability insurance. Because cyber incidents are typically not covered by general liability policies, an organization can use cyber insurance to supplement its technology risk-management efforts by transferring a portion of that risk onto an insurance company. Whereas the insurance industry has more than a century of loss data from fires and floods, cyber insurance is still a relatively young offering. As a result, there are certain assumptions involved in determining premiums. For example, many cyber insurers will conduct a vulnerability scan against an applicant's public-facing website, and then use the results as a proxy for how well the organization is managing its cyber risk. Many organizations outsource their websites to marketing companies, however, and do not have administrative responsibility for technical support of those sites. In such cases, scan results can foster inaccurate representations. Thankfully, cyber insurers are beginning to more diligently investigate applicants' cybersecurity postures before quoting premiums.

Finally, many organizations are subject to regulatory requirements with implications for technology security. HIPAA, DoD CMMC, and PCI-DSS are common examples, but there are many, and the number will only increase over time. The owners and managers of an organization must clearly understand which requirements apply and how to satisfy them. Penalties for noncompliance can be severe and can lead to an organization's demise.

KNOW YOUR SYSTEM

Most organizations have wired and wireless networks to which workstations, servers, printers, cameras, and seemingly countless other devices connect. Some of these might be owned and managed by the organization (e.g., company-issued laptops), and others might be employees' personal devices (e.g., smartphones). Since you need to know what you've got before you can protect it, use a discovery tool to identify which devices are connected—and where. This type of tool can actively scan the network, or it can passively collect data from switches and wireless controllers as devices connect. This helps to create a device inventory that is automatically kept up to date. Having such visibility into your network is a key piece of the cybersecurity puzzle.

Having visibility into your network is a key piece of the cybersecurity puzzle.

In environments with highly sensitive data or systems that should be accessible from only certain devices, an organization may wish to implement a solution for Network Admission Control (NAC). NAC integrates with switches and wireless controllers to restrict access to the network. It's typically configured to perform certificate-based authentication for laptops, smartphones, and other devices that connect. If a device has the proper certificate, it's granted full access to the network. Devices without a proper certificate can be automatically relegated to a restricted level of access (e.g., Internet only). In this way, the certificate is like a "golden ticket" that's required for full access. NAC prevents someone from connecting to the internal network from an unauthorized device.

NAC can also be used to ensure that employees' personal smartphones and tablets have been registered with the organization's Mobile Device Management (MDM) platform. With the influx of mobile devices and the sudden growth of mobile technology, more and more organizations are allowing employees to utilize their own devices to access corporate intranet, email, SharePoint, and more. Although this practice affords flexibility for the employee, it also poses significant security risks to the organization. If a device is lost or stolen, sensitive business data can wind up in the wrong hands, and unauthorized access to company systems can occur. An MDM platform extends organizational control to mobile devices that have access to company data. It allows an organization to control security parameters and permitted apps, compartmentalize and control company data, and wipe devices that are lost or stolen.

KNOW YOUR SOFTWARE

Just as with understanding which devices are connected to its network, and organization must understand what software is installed on those systems. Use a software inventory tool to track the operating systems and applications installed on employees' computers. This will help to identify machines with unauthorized, outdated, or missing software, which in turn will help the organization to improve the consistency and manageability of its installed software base. If possible, integrate the software inventory with the aforementioned device inventory to create a unified repository of all relevant inventory information.

Also ensure that all computers are running a currently supported operating system. The use of outdated operating systems like Windows XP, Windows 7, and Windows Server 2008 dramatically weakens an organization's ability to defend against cyberattacks. Patches and hotfixes are no longer developed or supplied for these operating systems, and as security researchers and hackers continue to discover new vulnerabilities, unpatched systems could negate the other protective controls that an organization has deployed. You're only as secure as your weakest link, and outdated operating systems create an awfully weak link.

> You're only as secure as your weakest link, and outdated operating systems create an awfully weak link.

If circumstances require that employees have administrative privileges on their systems, use an application whitelisting tool to prevent the installation of unapproved software. It's no surprise that many applications—particularly those in the realm of freeware and shareware—are malicious and are designed to steal data, mine cryptocurrency, provide backdoor access, or lead to other undesirable outcomes. Preventing users from installing such software is an important step in the effort to minimize your systems' attack surfaces.

MANAGE YOUR VULNERABILITIES

> In order to efficiently and effectively address vulnerabilities, an organization simply must have the ability to automate and control patches.

Both security researchers and hackers put a lot of time and effort into discovering vulnerabilities in systems and software. Researchers are interested in making vendors aware of flaws in their products so that they can be patched. Hackers, on the other hand, are interested in being able to exploit the discovered vulnerabilities in order to obtain unauthorized access, steal data, knock systems offline, or any number of other undesirable effects. It's a constant, never-ending race between the good guys and the bad, and we're caught in the middle.

For this reason, an automated patch management tool is perhaps the most important security control that an organization can deploy. In an environment with tens, hundreds, or thousands of computers, trying to patch systems manually is an exercise in futility. In order to efficiently and effectively address vulnerabilities, an organization simply must have the ability to automate and control patches. New vulnerabilities are discovered and announced every day, and since each one represents a potential chink in your organization's armor, automated patch management is a must-have. Organizations must also ensure that vulnerabilities in their systems are detected as quickly as possible so that they're patched before they're exploited. Use a vulnerability scanning tool to perform frequent (e.g., weekly) scans against all devices connected to the wired and wireless networks. This will corroborate that your patch-management efforts are working as intended and will also quickly identify any stragglers that are missing patches (e.g., a machine that is powered off every night and subsequently misses its patch window). This also is a useful way to detect unauthorized devices connected to the network. Finally, it can provide peace of mind for system administrators, as they'd now have objective evidence that systems are being patched correctly.

RESTRICT ADMINISTRATIVE PRIVILEGES

The principle of least privilege is a core component of any good cybersecurity strategy. It specifies that a user's account should possess only the privileges necessary for that user to perform his or her job, and nothing more. As a practical example, if Bob's job requires him to send and receive email, compose documents, and browse the Web, his account should be able to do these things, but should not be able to install or remove software, launch PowerShell scripts, or make domain-level configuration changes in Active Directory. Attackers know that users' accounts have often been granted unnecessary privileges, so after compromising one account, they can take advantage of this weakness to more easily compromise other systems on the network. Matching an account's privileges to its purpose won't diminish the user's experience but will minimize the account's attack surface. As a general rule, a typical user's account should not have local- or domain-administrator privileges.

> Matching an account's privileges to its purpose won't diminish the user's experience but will minimize the account's attack surface.

But what about the organization's IT administrators? They've been tasked with the ongoing maintenance and support of workstations, servers, infrastructure devices, and just about everything else connected to the network. Much of what they do requires administrative privileges. In this case, they should use accounts with standard user-level privileges for general tasks like email and Web browsing, and then transition into privileged accounts with elevated rights only for tasks that actually require them. Though in the end they'd be using different accounts to accomplish different tasks, they'd still be adhering to the principle of least privilege because the account in use would be matched to the task at hand. Here again, the objective is to minimize the scope and likelihood of damage if an account were to be compromised.

HARDEN SYSTEM CONFIGURATIONS

We've already mentioned the importance of automated patch management and vulnerability remediation in the effort to protect computers against cyberattacks. But we can also harden system configuration settings in order to make those systems even more resilient. On this front, CIS provides a wealth of invaluable guidance in its Configuration Benchmarks. Configuration-hardening guides are available for many different types of systems—workstations, servers, infrastructure devices, cloud services, and more. Now, not every hardening technique is appropriate for every environment. There are some that could potentially cause performance issues or impact system availability. But most of these recommendations can be readily incorporated into organizations' standard local security policy and Group Policy templates with no adverse effects. The end result will be that systems are protected to a greater degree than with patching and vulnerability management alone.

> Hardening system configurations is important for visibility, stability, and peace of mind.

And to make sure these configurations remain intact on systems throughout the network, use a system configuration management tool. This will provide IT administrators with a central console for managing and monitoring the configuration settings on workstations, laptops, servers, and other managed devices. In the fight against malware and other cyberattacks, configuration consistency is key. Being able to affirm that the configurations of every managed device conform to the organization's specifications for system hardening is important for visibility, stability, and peace of mind.

MONITOR YOUR LOGS

Nearly every device—workstation, laptop, server, firewall, router, IoT device, and more—connected to an organization's network is capable of providing some very useful logging data. This information can be the key to uncovering a cyberthreat hidden on the network. However, no organization possesses the manpower to manually review these logs in a timely, consistent manner. Use a Security Information Event Management (SIEM) tool to automatically collect and analyze systems' logs and generate alerts if suspicious events are found. This approach ensures that the process of log collection and analysis is automated, consistent, complete, and performed in real time. Manufacturers have invested significant resources in developing the logging capabilities within their products, so it behooves us to use this information to our advantage in the fight against cyberattacks.

> Appropriately sized SIEM platforms are not inexpensive, and they require ongoing tuning of rules and alerts in order to maximize value.

Alternatively, partner with a trusted Managed Security Services Provider (MSSP) to perform this function. Appropriately sized SIEM platforms are not inexpensive, and they require ongoing tuning of rules and alerts in order to maximize value. A good MSSP has already devoted significant resources to fulfilling these requirements. Further, MSSP technicians are likely to be experienced in incident analysis and can use this experience to your advantage.

PROTECT EMAIL AND WEB BROWSING

Email is far and away the most frequent method attackers use to breach their targets. The FBI estimates that while the average bank robbery nets $3,000, the average email heist nets $140,000. The former is high-risk and low-reward, while the latter is low-risk and high-reward. It should come as no surprise that this is where organized crime is now focusing its efforts.

Phishing techniques have become extremely sophisticated and can trick even the most vigilant of users. Ensure that all of your organization’s incoming and outgoing email is inspected to detect and block malicious links and attachments. Encrypt outbound messages that contain sensitive information. In addition, implement Domain Keys Identified Mail (DKIM) and Domain-based Message Authentication Reporting and Conformance (DMARC) to prevent your organization’s domain from being used in a phishing message’s spoofed “from” address. This will help to preserve the integrity of your organization’s brand and will reduce the likelihood of your employees falling prey to phishing messages that appear to originate from your own domain.

Approximately 95% of known ransomware strains require the ability to resolve malicious names in order to take hold, so this control is a highly effective countermeasure in the fight against ransomware.

Configure your email server to prepend an “external sender” warning banner to the top of every email message received from an external sender. This banner is intended to heighten employees’ suspicions about clicking embedded links or opening attachments, thereby invoking their security awareness (more on that later) to complement the existing technical security controls.

We all understand the importance of using a firewall to protect our systems from attackers on the Internet. But controlling our organization’s outbound traffic is every bit as important as controlling the inbound traffic. A DNS security service such as Cisco Umbrella will prevent your systems from being able to resolve and connect to malicious domains. Approximately 95% of known ransomware strains require the ability to resolve malicious names in order to take hold, so this control is a highly effective countermeasure in the fight against ransomware. In addition, it will provide enhanced visibility that makes it easier to identify machines that have been compromised.

Also ensure that all of your organization’s computers—both on-premises and remote—are protected by a URL filter with dynamic categorization. This control blocks access to the types of websites (e.g., adult, gambling, peer-to-peer file sharing, etc.) that your organization’s management wishes to disallow. Many of these sites can diminish employee productivity, create potential legal repercussions for your business, and furnish a pathway for malware to infect the network. Also consider blocking access to proxy-avoidance and remote-PC-access sites. The former can potentially be used by employees to bypass your URL filtering restrictions, and the latter can be used to allow ad-hoc remote access (by anyone) to employees’ computers. While there’s no one-size-fits-all URL filtering policy that meets the needs of every organization, blocking unwanted sites is a key step in preserving uptime and eliminating data loss.

DEFEND AGAINST MALWARE

Most organizations do not possess the resources they need in order to investigate and proactively hunt for abnormal behavior. They lack the ability to see beyond suspicious activity. Use an anti-malware and Endpoint Detection and Response (EDR) tool to provide advanced threat hunting, incident response capabilities, and continuous visibility. EDR is a software agent installed on individual computers. It provides immediate access to the most complete picture of an attack at all times, reducing lengthy investigations from days to minutes. This allows your organization to proactively hunt for threats, uncover suspicious behavior, disrupt active attacks, and address gaps in defenses before attackers can.

Complement your EDR with a network-based anti-malware tool. EDR software resides on the individual computers it protects, and network-based anti-malware resides on the gateway between an organization's internal network and the public Internet. From this vantage point it's able to inspect all files being downloaded from (or uploaded to) external websites, regardless of which computer is initiating the transfer. Because it's able to quarantine or block malicious files before they can be received, it's a valuable component in any organization's malware defense strategy. And given the sophistication of today's malware variants, defense-in-depth must be sacrosanct.

LIMIT ACCESSIBLE SERVICES

Just as your organization uses a perimeter firewall to control which servers and services are accessible from the public Internet, so too can it use a software firewall on its laptops, workstations, and servers to control which services are accessible from the internal network. Earlier we mentioned the importance of the principle of least privilege when allocating rights to accounts. Limiting accessible services is a similar concept—we want to make sure that our systems are reachable only on the services required for legitimate business purposes, and nothing else. For example, if your organization's DNS server doesn't also need to be an FTP server, make sure that it's not running an accessible FTP server service. Use a port-scanning tool to conduct frequent scans against the internal network to identify which services are accessible on which computers, and then disable any services that are found to be unnecessary. This will help to minimize the attack surfaces of the systems connected to the internal network.

> We want to make sure that our systems are reachable only on the services required for legitimate business purposes, and nothing else.

If your organization hosts any application servers on-premises or in the cloud, protect them with a web application firewall (WAF). This control filters, monitors, and blocks HTTP traffic to and from a web application. A WAF is differentiated from a regular firewall in that a WAF is able to filter the content of specific web applications while a regular firewall blocks or allows connections based on IP addresses, protocols, and/or ports. By inspecting HTTP traffic, a WAF can prevent attacks stemming from web application security flaws, such as SQL injection, cross-site scripting (XSS), file inclusion, and security misconfigurations.

BE ABLE TO RECOVER

Every organization needs to be able to recover its data in the event of inaccessibility or corruption due to cyberattack, intentional or accidental deletion, or any number of other availability-impacting circumstances. The owners of each dataset first need to determine the corresponding Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for that asset. RPO is the maximum allowable age of files that are recovered from backup storage for normal operations to resume. In other words, it specifies how “fresh” the backups need to be, which determines how frequently the backups need to happen. RTO is the maximum allowable downtime (i.e., absence of dataset availability) during the process of recovery of that asset. It determines how quickly the backups need to be able to be restored. Taken together, an organization’s IT department uses the RPO and RTO information to design and configure the appropriate backup measures. Note that it’s not up to the IT department to determine RPO and RTO; those are business decisions that must be made by those who own the datasets (the organization’s business units, for example).

No matter what data your organization is backing up, and no matter the associated RPO and RTO, always follow the *3-2-1 Rule*. This says to maintain at least *three* copies of each dataset (the copy you’re using, plus two backups). Store the backups on *two* different types of media, which reduces the likelihood of both backups being inaccessible during an outage. Finally, keep *one* of the backups in a different location, such as an offsite datacenter or cloud repository. In addition, because many modern ransomware variants intentionally seek out and encrypt network-connected backup repositories, ensure that at least one of your backups is in a physically disconnected, *offline medium* like magnetic tape. Yes, what’s old is new again, but it’s a great way to ensure that you’ve still got a backup to restore in the event you need it.

PROTECT THE BOUNDARY

Many modern firewalls include the ability to block connections to and from known malicious IP addresses and domains without having to manually blacklist them. As cybercriminals have become adept at using Domain Generation Algorithms (DGAs) and changing IP addresses on the fly, trying to manually block attackers’ IP addresses (i.e., the whack-a-mole approach) is no longer sufficient. Ensure that your organization’s perimeter firewall is capable of blocking traffic to and from known malicious IP addresses and domains, and that the corresponding blacklist is maintained and regularly updated by the firewall manufacturer. Also make sure that your firewall is configured to send a logging message to your SIEM in the event that a computer on the internal network attempts to reach a large number of such IP addresses or domains. This may be a telltale sign of a compromised machine, and the earlier it can be detected, the earlier it can be remediated.

Next, many modern firewalls include the ability to send NetFlow flows to an analyzer. NetFlow is a lightweight, efficient protocol that can be used for traffic-analysis and reporting purposes. It includes a wealth of information about inbound and outbound connections that have been allowed through the firewall. Use a NetFlow analyzer tool to collect and automatically assess this information. It can be critical in incident response and investigation efforts, as well as highlight suspicious traffic patterns that could indicate a compromised computer on the network.

Most modern firewalls also include some type of Intrusion Prevention System (IPS). This allows the firewall to make a block or allow decision based on the content of a packet, rather than just on the IP address, protocol, and/or port information. An IPS, for example, should be able to detect and block attacks like SQL injection and cross-site scripting (XSS), whereas those attacks would make it through a legacy firewall without IPS capabilities. Ideally the IPS should have some way to automatically determine which operating system and vulnerabilities exist on each computer on the organization's internal network. An attack designed to exploit an IIS vulnerability, for example, may be useless against a server running Apache, so accuracy of the IPS protection hinges upon knowing whether the target of an attack is truly vulnerable. For optimal results, ensure that your organization's IPS is of the "smart" variety.

Further, most modern firewalls support remote-access VPN connectivity to accommodate offsite employees and vendors. When provisioning remote-access VPN functionality, first create a list of all expected use cases (e.g., employees connecting from home, vendors connecting from their offices, etc.). For each use case, determine specifically which systems on the organization's network should be accessible, and then configure the VPN access privileges accordingly. This is another extension of the principle of least privilege and using it to ensure that a VPN-connected user can reach only the systems that he or she should be able to reach is another important step in minimizing the organization's attack surface.

And firewalls aren't just for your organization's physical facilities. Many vendors make virtualized versions of their hardware firewall appliances that can be deployed in public cloud environments such as AWS and Azure. If your organization hosts publicly accessible systems in the cloud, be sure to protect them with a virtualized firewall that performs the aforementioned functions. Otherwise, an attacker could have a clear shot at those systems and compromise them to steal data and infect the rest of your organization's network.

The Target breach of 2013 could have been prevented with proper network segmentation.

Finally, use network segmentation to group similar systems together on VLANs and corresponding IP subnets, and then restrict which network traffic is eligible to flow between those subnets. For example, if your organization has a network-connected device that is part of the building's HVAC system, put this device on a dedicated HVAC network, and then prevent it from being able to communicate with your servers, workstations, or any other systems with which it doesn't need to communicate. This is a great approach to securely accommodating the rapid influx of Internet of Things (IoT) devices like IP cameras, door locks, kitchen appliances, and myriad other endpoints. As a real-world example, the Target breach of 2013 could have been prevented with proper network segmentation.

PROTECT YOUR DATA

The first step is to know where your organization's sensitive data resides. Maintain an inventory of all sensitive information stored, processed, or transmitted by your systems, including those located on-premises or at a remote service provider. A number of vendors in the Data Loss Prevention (DLP) space have created computer- and network-based DLP scanners that can locate sensitive data throughout the environment. These tend to be expensive but depending on the organization's need for speed and accuracy in locating sensitive data, they may be the most effective tool for the job.

Maintain an inventory of all sensitive information stored, processed, or transmitted by your systems, including those located on-premises or at a remote service provider.

If your organization uses a cloud-based file-management service such as SharePoint Online or Google Drive, restrict the default and user-selectable sharing privileges for files and folders. Because this data resides in the cloud, the entire Internet-connected world has the potential to access it. Typical users aren't necessarily aware of the need to restrict access, so it's generally a good idea to make that decision for them. Many organizations, for example, restrict their users' default and selectable sharing privileges to allow access from only other users in that organization, rather than public or anonymous access from anywhere. This is a basic security measure, but unfortunately is one that's often overlooked.

Within Active Directory, shared network folders provide a valuable function, but over time the access permissions can spiral out of control. This creates unneeded security exposure because the shares are accessible by more people than those who actually need to use them. At a regular interval, use a tool such as AccessEnum to capture a "snapshot" of the existing network-share access matrix and then determine whether anyone's level of access needs to be modified or revoked. Here again, the goal is to match account privileges to actual requirements, and nothing more.

To preserve confidentiality in the event a laptop is lost or stolen, deploy full-disk encryption software wherever possible. Without disk encryption, a lost or stolen laptop presents the possibility of sensitive data loss. Microsoft has included BitLocker disk encryption with Windows 10, but it needs to be enabled centrally (via Group Policy). It is recommended that all mobile devices have BitLocker enabled and the encryption keys stored in Active Directory.

Many organizations elect to restrict the use of USB-connected external storage media on managed computers. The reason for this is twofold. First, a favorite tactic of attackers is to plant malware or backdoor access on a USB stick and leave it somewhere conspicuous (out in the parking lot, for example). Humans are curious by nature, so it's likely that someone will find it, plug it in, and then release the malware or backdoor into the environment. Second, organizations that wish to control the spread of sensitive data may want to prevent employees from writing files to removable media. Once company data has been copied to a USB stick, for example, the organization doesn't have much opportunity to detect or control it.

CONTROL WIRELESS ACCESS

Wireless LAN access has become nearly ubiquitous in today's office environment. Devices like smartphones, tablets, and many others don't even have wired capabilities. To accommodate, organizations have deployed wireless access points (APs) and controllers to provide coverage throughout their facilities. This is convenient, but it also creates significant risk for the organization if access isn't carefully controlled. Recall our earlier discussion about identifying use cases for remote-access VPN and restricting access accordingly. Organizations should take the same approach with provisioning wireless access. Decide which use cases (e.g., employees who need full access to the internal network, guests who need access to the Internet only, etc.) need to be supported, and then configure the wireless infrastructure to enforce those restrictions.

Many organizations use pre-shared keys (i.e., Wi-Fi passwords) to protect their wireless networks. These are simple to deploy but can be costly to maintain. If a user who knows the Wi-Fi password were to leave the organization, all wireless devices would need to be manually updated to use a new key, otherwise the departed user would still be able to connect to the wireless network if in proximity (like out in the parking lot). In addition, shared keys can be captured and cracked using free, open-source tools. Wherever possible, rather than using a singular shared key to authenticate wireless computers, incorporate 802.1X (EAP-TLS) to authenticate wireless users and computers individually. EAP-TLS authentication replaces the shared key with per-user and -device digital certificates. This helps to ensure that only authorized users and devices are able to connect to the wireless network and eliminates the need for manual key changes following the departure of an employee who knows the Wi-Fi password. In addition, it allows the organization to control Wi-Fi access on a per-user basis.

Many modern APs include wireless intrusion detection system (WIDS) capabilities. In addition to detecting and blocking suspicious traffic from devices connected to the wireless network, some of them are able to suppress radio signals from rogue APs. One of the major challenges that organizations face on the wireless front is that well-intentioned (or otherwise) employees bring their own Wi-Fi routers from home and plug them in under their desks. As you can imagine, this creates a pathway that completely bypasses the organization's other security controls and may allow an attacker in proximity to obtain full, unrestricted access to the internal network. Detecting and suppressing rogue wireless networks is a critical capability here.

MONITOR AND CONTROL ACCOUNTS

Implement multifactor authentication (MFA) and use it everywhere it's supported, but particularly in conjunction with publicly accessible services such as Office 365, SharePoint Online, remote-access VPN, and the organization's DNS administration portal. Any computer in the Internet-connected world could conceivably attempt to log into these services, and traditional passwords do not provide a sufficient level of protection. Many users reuse their Active Directory account passwords for their personal accounts on other websites, and if an attacker were to breach a site and obtain those credentials, he or she could use them to obtain access to the organization's systems or mailboxes. In addition, a user could easily fall prey to a phishing attack and disclose his or her credentials in response. In certain situations, MFA can be defeated by a resourceful attacker, but it's still much better than using passwords alone to prevent unauthorized access. Many vendors offer tried-and-true MFA solutions, and more and more systems support MFA integration every day.

Incorporate a process to ensure that a user's accounts are disabled immediately upon termination of employment, and that any shared- or service-account passwords known by that user are changed. Each of these represents a chink on your organization's armor, and as soon as someone is exited, the race is on to close the holes before they're exploited. Also incorporate a recurring process to identify and disable accounts that are dormant and/or no longer needed. Finally, configure your SIEM to alert when it detects login attempts from disabled accounts. This can be an early indicator of an attack in progress.

By eliminating the need for users to remember and manually enter their passwords, a password manager aids employees' security awareness and provides a great complement to MFA.

Use a password manager tool to give your IT administrators and other employees the ability to generate complex, unique passwords for each of their accounts and to store them securely. This will reduce the likelihood of credential theft due to phishing attacks, weak passwords, or password reuse. By eliminating the need for users to remember and manually enter their passwords, a password manager aids employees' security awareness and provides a great complement to MFA.

SECURITY AWARENESS TRAINING AND TESTING

All employees should receive security awareness training on a frequent, recurring basis. As the human factor tends to be an organization's weakest link in its cyber defense, ensuring that your employees are working with (rather than against) your existing security controls is critical. Many vendors provide short, video-based training modules about such timely security-awareness topics as using secure authentication methods, identifying social engineering (e.g., phishing) attacks, safe handling of sensitive data, causes of unintentional data exposure, and the proper way to identify and report potential security incidents. Upon conclusion of a training module, participants are typically required to pass some type of quiz to gauge comprehension and retention of the material. Alternative forms of training include in-person and virtual instruction, but as a matter of convenience, the on-demand, video-based variety has become popular.

Supplement your organization's training efforts with recurring tests such as phishing campaigns. This will serve as a practical demonstration that employees' security awareness is improving. Initial results (click rates) of the phishing campaigns are likely to be substandard, but as employees realize they're being tested on a frequent, recurring basis, results should dramatically improve. Many organizations have fostered an environment of security awareness through positive, public recognition of employees who score well on their phishing tests. Nobody likes to be seen as a weak link, so a bit of healthy competition in these campaigns can pay dividends across the board.

RESPOND TO INCIDENTS

It's really not a question of "if" your organization will experience a cyberattack, but "when." When an incident occurs, it's too late to develop the procedures, reports, responsibilities, legal protocols, and communications strategy that will allow you to manage the cyberthreat and recover. Without an incident response plan (IRP), an organization may not discover an attack in the first place. Or, if an attack is detected, the organization may not follow sound procedures to contain damage, eradicate the attacker's presence, and recover in a secure fashion. Thus, the attacker may have a far greater impact, causing more damage, infecting more systems, and potentially exfiltrating more sensitive data than would otherwise be possible were an effective IRP in place.

> Practicing incident response is a great way for an organization to keep its employees sharp and ready to jump into action should a real security incident materialize.

Develop and document an IRP that defines standard procedures, roles and duties, and key management personnel with decision-making authority. Define organization-wide standards for employees to report anomalous events to the incident handling team, the approved methods for such reporting, and the kind of information that should be included in the incident notification. Document third-party contact information to be used to report a security incident, such as law enforcement, relevant government departments, vendors, and Information Sharing and Analysis Center (ISAC) partners. Also incorporate the incident-response process into your organization's security awareness training program so that all employees are familiar with it.

On a recurring basis, conduct mock incident response exercises and include employees who have roles in the response process. These can be conducted as tabletop exercises for hypothetical scenarios and should help participants to maintain awareness and comfort in responding to real-world threats. Exercises should test communication channels, decision making, and the incident responders' technical capabilities using the tools and data available to them. Practicing incident response in this manner is a great way for an organization to keep its employees sharp and ready to jump into action should a real security incident materialize.

PENETRATION TESTING

The preceding sections of this guide discuss many administrative, procedural, and technical security controls. Each is designed to counteract a specific type of cyberthreat. In theory, the more security controls that an organization implements correctly, the better it will be protected. But that raises a couple of important questions. How can you be sure that your organization's controls have been implemented correctly, and are there gaps in its protections? These questions are precisely what a penetration test is designed to answer.

Conduct recurring penetration tests to identify and exploit vulnerabilities in your organization's systems and software. Think of these as practical demonstrations that your organization's security controls are doing (or failing to do) what you think they are. The results of a penetration test provide deeper insight—through demonstration—into the business risks associated with various vulnerabilities. Use them to corroborate and improve upon your organization's cyber defenses.

CONCLUSION

This guide highlights many administrative, procedural, and technical security controls that mitigate cybersecurity threats faced by organizations today. But cybersecurity is a never-ending process of continuous improvement, not a destination at which your organization can suddenly arrive. There's no magic cybersecurity bullet, so defense in depth is the only viable strategy for surviving in today's threat landscape. Implementing the recommendations in this guide will not protect against every threat but will allow your organization to keep from being low-hanging fruit in the metaphorical attack orchard. And given the choice between an unprotected target and one that is well protected, attackers will go after the former nearly every time.

Corsica Technologies partners with organizations to help them meet the standards for Cybersecurity Resilience. ***Schedule an appointment*** today with one our cybersecurity experts to learn more or contact us for a ***Risk Assessment***.

corsica technologies

Leadership | Commitment | Experience