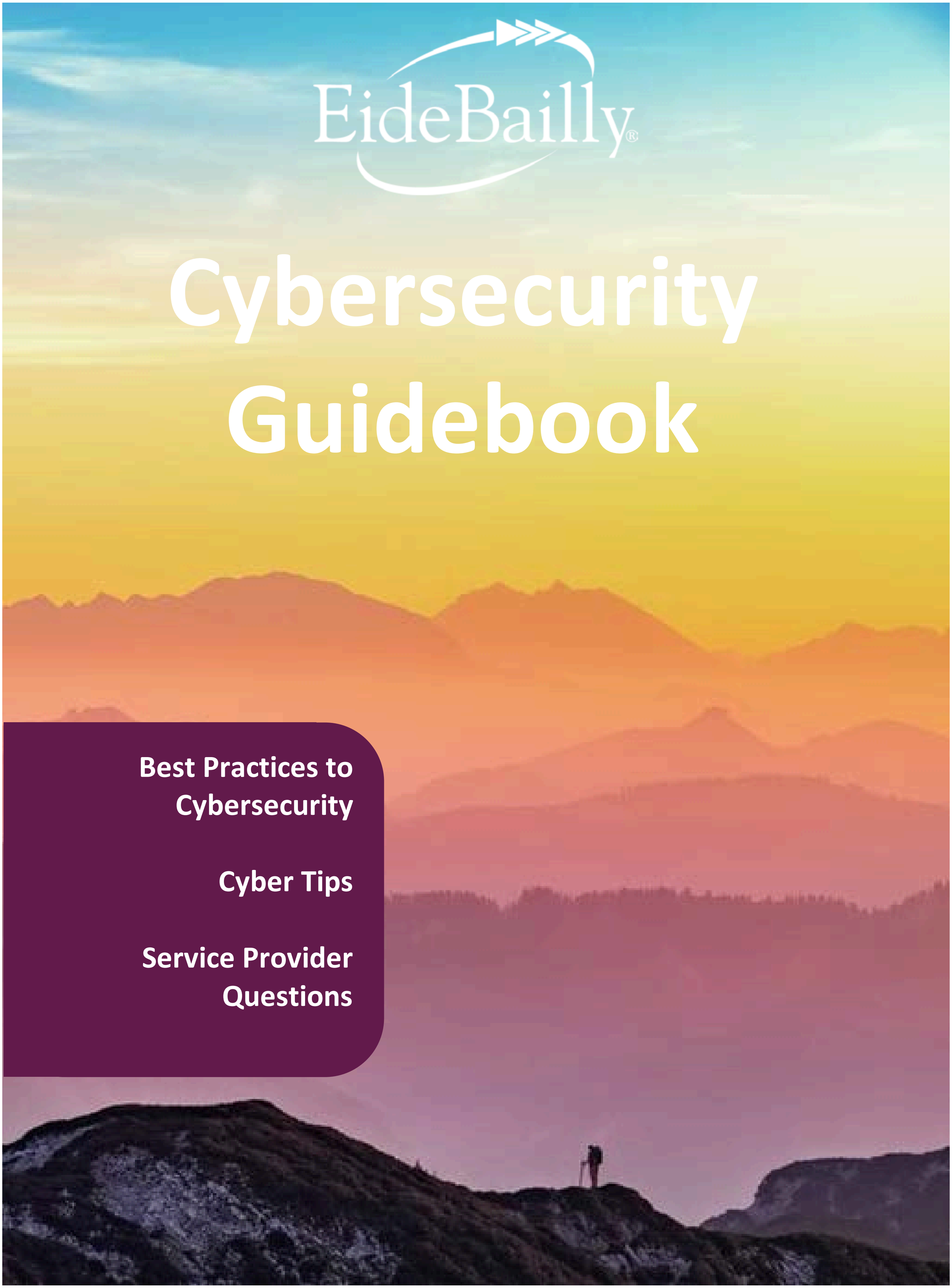


EideBailly®

Cybersecurity Guidebook

Best Practices to Cybersecurity

Cyber Tips

Service Provider Questions

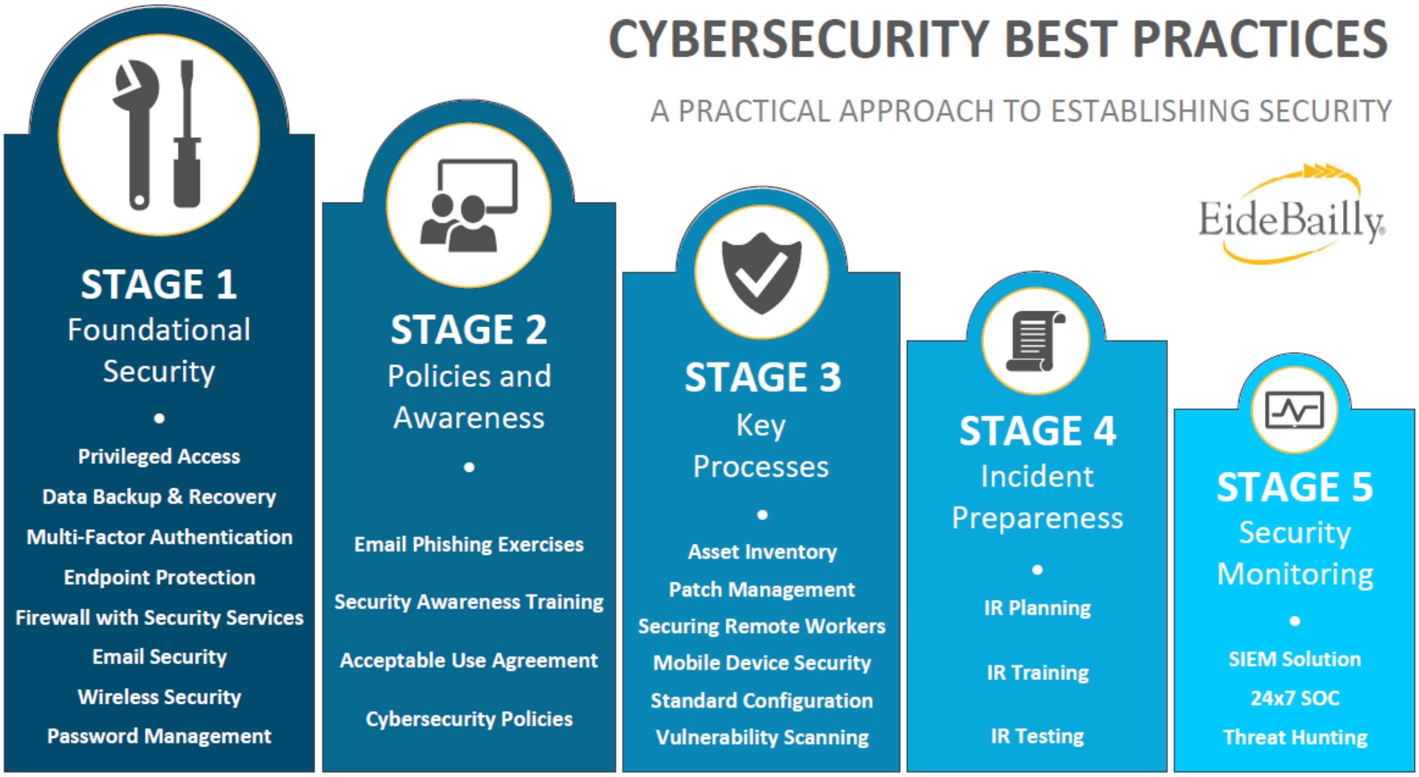
Table of Contents

Cybersecurity Guidebook

At some point, each organization will undergo a security transformation – adopting a new vision that places accountability for cybersecurity with the leadership team and responsibility for cybersecurity with everyone. The key is to adopt this new vision ***before*** and not ***after*** an attempted data breach. While most organizations recognize the need for good cybersecurity, they often struggle knowing what that looks like or where to start. This Cybersecurity Guidebook provides a practical approach and instructions for implementing cybersecurity best practices at any organization.

Your data has never been more at risk than it is today. The costs of a cybersecurity incident (both financial impact and reputation) have never been greater. Cyberattacks are the fastest growing crime in the US, and they are increasing in size, sophistication and cost. The current average cost per cyberattack on businesses is $380K per incident. Ransomware, the fastest-growing type of cybercrime, will claim a new victim every 5 seconds by 2021. Eighty-three percent of data breaches against small businesses are financially motivated.[1] Cybersecurity encompasses the people, processes, and technologies that protect your personal information, intellectual property, high-value data, and information systems from theft or damage by criminals and adversaries.

This Guidebook provides instruction for small and medium sized organizations on a practical approach to implementing best practices in cybersecurity. This approach is broken up into five stages with specific steps to follow in each stage. Following each step in the order, they are presented is not necessary, but we have organized the stages to the first address preventative measures that would protect against the most common attacks we have seen.



CYBERSECURITY BEST PRACTICES

A PRACTICAL APPROACH TO ESTABLISHING SECURITY

EideBailly

STAGE 1
Foundational Security
•
Privileged Access
Data Backup & Recovery
Multi-Factor Authentication
Endpoint Protection
Firewall with Security Services
Email Security
Wireless Security
Password Management

STAGE 2
Policies and Awareness
•
Email Phishing Exercises
Security Awareness Training
Acceptable Use Agreement
Cybersecurity Policies

STAGE 3
Key Processes
•
Asset Inventory
Patch Management
Securing Remote Workers
Mobile Device Security
Standard Configuration
Vulnerability Scanning

STAGE 4
Incident Preparedness
•
IR Planning
IR Training
IR Testing

STAGE 5
Security Monitoring
•
SIEM Solution
24x7 SOC
Threat Hunting

[1] Statistics from Cybersecurity Ventures, Accenture, Hashedout, EY

The sections that follow provide instruction and guidance for the steps in each stage of the approach outlined in the diagram above. Each step is a specific security control activity that is presented in the following format:

- **Overview**
    - The *Overview* section provides a high-level explanation of the security control.

- **Why are they important?**
    - This section explains why the control is important to an organization's overall cybersecurity program and protection of its data.

- **Configuration**
    - The *Configuration* section provides action items for each security control that can be implemented to improve or ensure an organization's cybersecurity. We provide three implementation tiers, depending on your organization's size, risk appetite, and maturity
        - Essential, at the bare minimum an organization should be doing these
        - Better, for organizations who may be a bit more mature or just want to do more to protect their organization
        - Optimized, best practices for organizations to provide the best protection concerning a specific control.

      Each tier has a corresponding act list. The tiers build on one another. For example, it's best to ensure everything in the *Essential* tier is implemented before moving on to security controls in the *Better* tier.

    - Each security control can be implemented independently, meaning if you want to follow the *Better* tier for one control but *Essential* for another, that is all right.

Essential	Better	Optimized
• Setting 1	• Setting 2 • Setting 3	• Setting 4 • Setting 5 • Setting 6
To Do	**To Do**	**To Do**
☐ Action item 1	☐ Action item 2 ☐ Action item 3	☐ Action item 4 ☐ Action item 5 ☐ Action item 6

- **Managed Service Providers (MSP) Questions**
    - Outsource your IT? No problem, each section has reference to specific questions about the security control that you can ask your managed service provider to get a better understanding where your risks might reside.

STAGE 1 - Foundational Security

Step 1 Privileged Access

Overview

Privileged accounts are accounts with higher access to an organization's information systems than general users. Organizations may have privileged accounts within specific applications, devices, or even across the entire network.

Why are they important?

Statistically, most cybercrimes involve privileged access to organizations resources. Limiting and monitoring privileged accounts can significantly reduce the risk to the organization.

> *Just by preventing access to privileged accounts, an organization could safeguard all the computers and prevent attackers from exploiting 94% of all the critical vulnerabilities Microsoft patched during the past year. (BleepingComputer)*

Configuration

Because privileged users have so much power, most organizations have some basic controls in place to limit or audit their activity. But are you doing everything you should? Here are the best practices you can follow to take control of privilege users across your environment.

Essential	Better	Optimized
• End-users are not local administrators on endpoints. • Users with privileged accounts are setup with two accounts (one for day to day, the other is the privileged account for tasks requiring elevated tasks).	• Privileged accounts have a more stringent password requirement. • Privileged accounts require multi-factor authentication. • Privileged accounts are documented, reviewed, and approved by leadership.	• Activities of privileged accounts are tracked and auditable. • Privileged accounts are setup with least privilege. • Local Administrator Password Solution (LAPS) implemented. • Privileged Access Management (PAM) solution implemented.
To Do	**To Do**	**To Do**
□ Remove or ensure end-users are not setup as local administrators on their workstation or laptop. □ Setup separate privileged and day-to-day accounts for users who require privileged accounts. □ Educate users when to use privileged account vs day to day account.	□ Setup privileged accounts with stricter password requirements (e.g. 16+ minimum character length, lockout policy of 3, required to change every 90 days). □ Enable multi-factor authentication for privileged accounts. □ Create and maintain a list of all privileged accounts. □ Create a formal privileged account processes (e.g. when privileged accounts should be used, approval process for new privileged accounts, periodic	□ Enable or configure systems to record privileged activity (e.g. account access is elevated, passwords changed, logon/ logoff, etc.). □ Configure privileged accounts to bare minimum privileges needed for their responsibilities (e.g. only reset passwords but can't change system configurations). □ Implement Microsoft's Local Administrator Password Solution (LAPS) to manage local administrator accounts. □ Review the use case for privileged access management

	reviews to ensure access is still required).	(PAM) solution within the environment.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning privileged access. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Do you setup users within our organization with local admin rights?	No, local administrator accounts/ passwords are not provided to end users.	Yes, users are setup as local administrators.	Administrative access allows users to install or remove software (including safeguards) and reconfigure system settings. This significantly increases the likelihood of malware and ransomware.
How do you manage our organization's credentials or access to our resources?	MSP utilizes a password manager or privileged access manager (PAM) for storing and using your organization's passwords.	MSP utilizes a spreadsheet or stores credentials in emails.	If your MSP doesn't properly manage the credentials, they use to access your resources, your environment could be compromised. You'll want to clearly understand how they protect and manage credentials.
How do you manage the separation of your employees? How do you confirm a former employee can't access our resources?	MSP has a formal separation process that includes disabling separated user's accounts in a timely manner and changing service account passwords for all your organization's resources.	MSP has no formal separation process and passwords are not changed after a separation.	If your MSP doesn't change user passwords after a separation, there is a chance that a separated employee may remember a password and use it to access your organization's resources. This is especially true for resources in the cloud (e.g. Office 365, Salesforce, etc.)

STAGE 1 - Foundational Security

Step 2 Data Backup & Recovery

Overview

Backing up data is the act of making copies of your organization's essential data and storing those copies at different locations. Recovering is the ability to retrieve the backups and restore the data to production.

Why are they important?

In an event where data is lost, an organization often needs to recover the lost data to regain normal operations. Data could be lost for several reasons including hardware failure, user error, ransomware, etc.

> *Ninety-three percent (93%) of companies that lost their data for 10 days or more filed for bankruptcy within one year of the disaster, and 50% filed for bankruptcy immediately. (National Archives & Records Administration in Washington DC.)*

Configuration

Losing information can be devastating for an organization. Are you doing everything you should to ensure your most valuable data is backed up? Here are the best practices you can follow to ensure your organization's data is properly backed up.

Essential	Better	Optimized
• Conduct daily backup of all data that is essential to your operations. • Maintain a copy of your data backups offsite (e.g. cloud or different facility).	• Follow the 3-2-1 backup strategy: **3** copies of all data on **2** different types of media (e.g. disk & tape) **1** copy stored offsite. • Implement a strategy to ensure a copy of all data is stored offline (i.e., cold storage). • Perform random testing of backups. • Educate appropriate users on the organization's backup strategy.	• For business-critical data, ensure backups are performed on an hourly basis. • Develop and implement a formal Archival Plan and/or Data Retention Policy. • Conduct annual Disaster Recovery testing and training exercises.
To Do	**To Do**	**To Do**
☐ Perform an analysis to identify the data that is critical to your organization's operations. ☐ Implement an automated backup strategy to duplicate data or develop a manual process to duplicate data daily. ☐ Store a copy of backups offsite (e.g. Cloud or different facility).	☐ Implement a backup solution to schedule and manage backups ☐ Ensure backups follow the 3-2-1 rule. ☐ Ensure a copy of all data is maintained in cold storage. ☐ Quarterly test backups to ensure data is retrievable and all data is properly being backed up. ☐ Educate appropriate users on the frequency of backups, what data is backed up, and restoration processes.	☐ Identify any data that needs to be backed up more frequently than daily, and adjust backup processes and/or procedures accordingly. ☐ Implement a formal archival plan for backups or follow organizational retention policy for ensuring ample backups are maintained. ☐ Annually test backups as part of a full disaster recovery testing. Ensure backups are recoverable in a cloud environment or on different hardware.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider backups. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
How often is our data being backed up? And Where is it stored?	Data is backed up at least daily and stored in multiple locations (e.g. in organizations facility, and another copy in the cloud).	Data backups are only done weekly, and/ or backups are stored on the same hardware that the data resides.	Without proper backups, data could be lost or become corrupted, crippling an organizations ability to function

How is our data and backups protected against ransomware?	Multiple copies of backups are maintained with at least one being offline to ensure they can't be encrypted.	No offline storage of backups and MSP utilizes the same backup instance for all clients.	Without offline or cold storage backups ransomware may encrypt not just live systems but all backups rendering them useless. Without proper controls or physical separation, backups are just as likely to become encrypted during a ransomware attack.
Are backups of our data ever tested to ensure its complete and recoverable?	Backups are periodically tested to ensure the data is properly backed up and recoverable.	Backups are never tested.	The worst time to find out that backups are not complete or corrupt is after a security incident. Without proper testing, backups may not be complete or recoverable.

STAGE 1 - Foundational Security

Step 3 Multi-Factor Authentication (2nd Factor)

Overview

Multi-factor authentication is a security authentication method that verifies users identify by requiring multiple identifiers. Multi-factor consists with at least two of the following three identifiers: something you know (e.g., password or pin), something you have (e.g., phone or token), and something you are (e.g., fingerprint, retina scan)

Why are they important?

Multi-factor authentication provides a second layer of protection in the event a user's password is lost or stolen.

Fifty percent (50%) of users use the same password for all accounts (Global Password Security Report).
Multi-factor authentication can block over 99.9% of account compromise attacks (Microsoft).

Configuration

Account compromise can have multiple effects on an organization. Are you doing everything you should to ensure your organization's accounts are protected from compromise? Here are the best practices you can follow to ensure accounts are properly protected.

Essential	Better	Optimized
• Require multi-factor authentication for access to email and VPN (remote) accounts.	• Require multi-factor authentication for access to all the organization's externally facing resources. This includes hosted solutions (e.g., Software as a Service). • Require multi-factor authentication for access to all the organization's privileged system accounts.	• Require multi-factor authentication for access to any highly sensitive information (e.g. classified information, medical records, financial data, proprietary information). • Utilize a centrally managed identity and access management (IAM) tool to manage authentication including multi-factor. • Utilize more secure forms of multi-factor authentication (e.g.,

		biometrics, authenticator app, or keyfob).
To Do	**To Do**	**To Do**
☐ Enable multi-factor authentication on the organization’s email service. ☐ Enable multi-factor authentication for VPN service or any other types of service that provides external access to internal resources.	☐ Create and maintain a list of tools, solutions, and services that are accessible externally to your organization’s internal network. ☐ Enable multi-factor authentication on all externally facing resources. This includes hosted solutions (e.g., Software as a Service). ☐ Enable multi-factor authentication for privileged accounts.	☐ Create and maintain a list of all applications or storage repositories that house or process sensitive information. ☐ Invest in an IAM tool to manage authentication for internal and external resources. ☐ Do not utilize SMS (text) messaging as the second form of authentication. Instead, utilize a more secure form of multi-factor authentication (e.g., biometrics, authenticator app, or keyfob).

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning multi-factor authentication. We’ve also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Does your company utilize multi-factor authentication when accessing our organization’s resources?	MSP requires multi-factor for all its personnel to access your internal resources or hosted solutions (e.g. Office365).	Multi-factor is not required to access your organization’s resources by your MSP.	Managed Service Providers are substantial targets for cybercriminals since they have access to so many different organization resources. If credentials of the service provider become compromised your organization’s data may be at risk. Multi-factor authentication can help provide another layer of defense in these types of events.
Is multi-factor authentication enabled for all external resources?	MSP configures your external resources like VPN, Office365, Salesforce with multi-factor authentication for all your organization’s users.	MSP has not enabled or discussed enabling multi-factor authentication for externally facing resources.	Account compromise is one of the leading cyber threats to organizations, and multi-factor authentication can greatly reduce the likelihood of an account compromise.

STAGE 1 - Foundational Security

Step 4 Endpoint Protection

Overview

Endpoint security usually refers to an application that detects and blocks malicious software. Some endpoint tools can also provide data loss prevention, encryption, firewall functionality, and application whitelisting.

Why are they important?

The definition of an "endpoint" has expanded to more than just a workstation at a desk. Laptops, smartphones, tablets are all now considered endpoints that need to be monitored and protected if they are being used to access corporate data. Ensuring all endpoint devices are protected provides the organization with another layer of protection from malicious software, insider threats, and more.

> *Seventy percent (70%) of all breaches still originate at endpoints. (International Data Corporation)*

Configuration

Most incidents originate at an endpoint. Are you doing everything you should to protect endpoints from compromise? Here are the best practices you can follow to ensure endpoints are properly protected.

Essential	Better	Optimized
• Require Windows Defender to be enabled on all Window devices. • Require Windows Firewall to be enabled on all Window devices. • Require all endpoint devices to encrypt data at rest.	• Require use of a next-generation endpoint detection tool. • Deployment and monitoring of next-generation endpoint detection tool are centrally managed. • Installed next-generation endpoint detection tool on all devices, not just Windows devices. • Require active alerting to be enabled and configured.	• Endpoint tool is actively monitored or imported to SIEM. • Active reporting is provided to leadership. • Regular audits are conducted to ensure the endpoint tool is properly configured and installed on all devices. • Block USB access to all users without justification. • Centrally manage full disk encryption configurations. • A Data Loss Prevention (DLP) tool is utilized.
To Do	**To Do**	**To Do**
□ Enable or ensure Windows Defender with Real-Time protection is enabled. (Window Security > Virus & Threat Protection > Manage Settings > Real-time Protection). □ Enable or ensure Windows Defender with Real-Time protection is enabled. (Window Security > Firewall & network protection).	□ Deploy a next-generation endpoint detection tool that can run on multiple operating systems (e.g. Windows, Mac, Linux). Examples of a next-generation tool are Crowdstrike, Cylance, and SentinelOne □ Ensure that the endpoint tool can be centrally managed. □ Install the endpoint tool on all devices including servers, mobile	□ Create procedures to actively monitor activity on the endpoint tool or import logs to SIEM product. □ Create formal, documented processes to engage leadership on the activity seen on endpoints. □ Perform quarterly audits to ensure the endpoint detection tool is installed on all devices and

☐ Enable BitLocker on all Windows devices to encrypt the entire disk. ☐ Enable FileVault on all Mac devices to encrypt the entire disk.	devices, workstations types (e.g., Windows, Linux, Mac, etc.). ☐ Configure the endpoint tool to alert key personnel when something is detected.	properly communicating to the management console. ☐ Configure systems to block USB storage devices. ☐ Configure Windows systems to enroll BitLocker encryption keys with Active Directory. ☐ Configure endpoints with a DLP tool that monitors for sensitive data being saved locally on devices or being sent outside of the organization.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning endpoint detection tools. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Does your company monitor the endpoint tool and alert us if something is found?	MSP receives alerts when something is detected by the endpoint and investigates to determine where it originated and ensure it's been blocked or eradicated.	MSP sets up the endpoint tool but does not perform monitoring. Takes the mentality it will block anything it deems malicious.	Set and forget is a bad approach to endpoint detection tools. If something is blocked or quarantined it might be a sign of a larger issue and should be investigated.
Does your endpoint monitoring tool meet our needs?	MSP has options when it comes to endpoint detection tools. Each comes with benefits and costs. A good service provider will discuss these with you and help find a tool to meet your needs.	MSP only has one option for endpoint detection tools.	Having an endpoint detection tool is important; however, deciding which product to use should be based on an organization's needs and product features (e.g. automation, customizations, data loss prevention, phishing detection, agent vs agentless, compatibility, and integrations). Cost and the type of data you manage should also be considered when deciding on an endpoint detection tool.

STAGE 1 - Foundational Security

Step 5 Firewall with Security Services

Overview

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet. Security services for a firewall include intrusion protection, application proxy, connection monitoring, and more.

Why are they important?

Firewalls by themselves can prevent many intrusions. However, to get the greatest benefit from a firewall, it must have services enabled that can identify intrusions and detect running applications. Firewall services are necessary to stop most threats today.

> *Twenty percent (20%) of all web traffic in 2018 had bad or malicious bots designed to create automated attacks on websites, web application programming interfaces (APIs), and mobile applications. (Distil Networks)*

Configuration

Firewalls tend to be the first defense against outside attacks. Are you doing everything you should to make sure your firewall is configured correctly? Here are the best practices you can follow when configuring your organization’s firewall.

Essential	Better	Optimized
• Utilize a firewall with Intrusion Prevention System (IPS) capability. • Configure your firewall to monitor and/or block all incoming AND outgoing traffic.	• Utilize a next-generation firewall. • Develop and maintain documented firewall rules. • Develop and implement an application blocklist/allow list. • Implement geo blocking on the organization’s firewall(s). • Implement URL filtering on the organization’s firewall(s). • Institute a formal plan and process for implementing changes to firewall configurations. • Implement standards for the retention of firewall logs. • Implement TLS inspection on the organization’s firewall(s).	• Monitor/ Important to Security Information and Event Management (SIEM) tool. • Conduct regular firewall security audits. • Life-cycle management process defined.
To Do	**To Do**	**To Do**
□ Install a firewall between the organization’s internal network and any external, untrusted network (i.e., internet). □ Configure the organization’s firewall to enable Intrusion Prevention System (IPS) functionality. □ Configure all externally bound (i.e., outbound or egress) traffic and all internally bound (i.e., inbound or ingress) traffic to go through the firewall.	□ Install a next-generation firewall with the capability of performing more than just port/protocol inspection. □ Establish a process to formally maintain a documented list of rules (i.e., configuration settings) for the organization’s firewalls. □ Enable or configure an application blocklist or allow list on the organization’s firewall to ensure only approved services are utilized (e.g. block storage	□ Actively monitor or import firewall logs to a SIEM. □ Conduct quarterly reviews of firewall rules to ensure they are properly configured and still needed. □ Create and institute a firewall life-cycle management process to ensure firewalls are kept up to date and on supported versions.

□ Consider the types of information that should be allowed to leave your network and configure the firewall to monitor outbound traffic and stop sensitive or suspicious information from leaving.	sites like DropBox if there is not an approved business need). □ Configure the organization's firewall to block traffic from countries you do not do business with (e.g. China, Russia, etc.). □ Configure the organization's firewall to block known bad web categories (e.g. gambling, malicious, adult content, etc.). □ Establish a formal change control process for documenting, tracking, and approving all changes to configuration of the organization's firewall. □ Develop and implement standards for ensuing the organization's firewall logs are being generated and stored. □ Enable secure TLS (https) inspection to monitor secure websites.	

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning a firewall. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Is our firewall a next-generation firewall that utilizes application inspection, intrusion prevention, and threat intelligence?	Your firewall is a next-generation firewall utilizing all of the features like application inspection, intrusion prevention, and threat intelligence.	Your firewall is a stateless firewall designed to protect networks based on static information such as source and destination.	Next-generation firewalls can correlate data and provide much more granular inspection of traffic vs older stateless firewalls that rely on source and destination traffic.
How far back do firewall logs go back?	Three or more months of logs are kept in case of an incident that needs to be investigated. Also, log retention is determined by date not size.	Firewall log retention is based on size, so the retention fluctuates meaning if traffic increases the furthest backlogs decreases.	Having the ability to go back and review firewall logs is essential when investigating an incident. If logs are not kept or complete it can greatly decrease the investigation process.
Are you actively monitoring the firewall for attacks or anomalies? Or is it a	Firewall generates alerts of persistent attacks and anomalies or the firewall traffic is	Firewall is setup initially and is never monitored or changed. Only monitoring if the	Like most technology just setting something up and expecting to never monitor or change will become less effective over time.

set it and forget mentality?	routinely monitored for persistent attacks and anomalies.	firewall is up and running.	

STAGE 1 - Foundational Security

Step 6 Email Security

Overview

Email security is composed of different controls to secure organizational email. These include accessing email mailboxes, preventing phishing, malicious code and spam, and preventing loss of data.

Why are they important?

Email security can prevent most attacks from reaching their intended recipients, which, in turn, reduces the number of successful compromises of hosts, user credentials and sensitive data.

> *Ninety four percent (94%) of all malware delivered in 2018 was delivered via email. (Verizon Data Breach Investigations Report)*

Configuration

Emails tend to be the easiest ways to infiltrate an organization. Are you doing everything you should to make sure your email service is configured securely? Here are the best practices you can follow to ensure your organization's email system is properly secured.

Essential	Better	Optimized
• Utilize antivirus, antispam and anti-phishing technologies. • Require multi-factor authentication on external email access. • External warning banner on all emails originating outside of the organization. • Automatic forwarding is not allowed. • Sufficient logging is enabled.	• Enable secure or encrypted email capabilities. • Utilize blocklist and allow list. • Require DKIM (DomainKeys Identified Mail). • Enforce TLS for a secure connection between sender and recipient.	• Monitor/ Important email system or gateway logs to SIEM. • Utilize an attachment sandbox when receiving attachments. • Utilize Data Loss Prevention (DLP) functionality within email to ensure sensitive data (PII, credit card numbers, etc.) are not being sent out unsecured.
To Do	**To Do**	**To Do**
□ Enable antivirus, antispam, and anti-phishing technologies within email service or email gateway. □ Enable multi-factor authentication on accessing email outside of the internal network. □ Configure email service to warn users when an email is from an external resource and to use	□ Enable or configure the ability to send secure emails to recipients outside of your organization. □ Don't configure your organization's domain as an allowed domain to bypass spam filters. □ Setup DomainKeys Identified Mail (DKIM) standard to help prevent spoofing on outgoing	□ Import email logs to a SIEM tool to alert on failed logins, excessive sent messages, sensitive information, insider threat, etc. □ Utilize a tool or service to open and inspect attachments securely in a sandbox environment. □ Enable data loss prevention capabilities to scan outgoing emails for credit card numbers,

caution when responding or opening attachments. ☐ Disable the ability to automatically forward emails to an external email address (e.g. all your work emails are forwarded to your personal Gmail account). ☐ Enable or ensure logging for email service is sufficient. This should include at least three months of successful and failed logins.	messages sent from your domain. ☐ Configure TLS by default for creating a secure connection between sender and recipient.	social security numbers, and other sensitive information.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning email security. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Does our email service have ample logging functionality?	Mailbox auditing actions are enabled.	Logging or auditing is not done or only kept for a very short time (e.g. 7 days)	Business email compromise is one of the most common types of incidents and without ample logging determine who got in and what was accessed is nearly impossible.
Are we doing everything to stop spam, malicious emails, and phishing attempts?	An additional service is used to stop/ prevent email like Microsoft ATP, Mimecast, or Proofpoint. These services sit in front of your email system and provide another layer of protection.	No additional service to stop or prevent malicious email is utilized other than what is offered with basic accounts.	While many services offer basic spam and malicious email prevention. Many times, additional services can provide greater protection.
If we receive suspicious emails can we easily submit them to you to review to determine if they are legit or malicious?	Your managed service provider offers a button within your email client that you can submit emails directly to them for review.	If an email passes all the technical safeguard it's up to the organization to determine if it's legitimate.	Sometimes emails pass all the technical safeguards. It's good to educate users on what to look for and be able to submit suspicious emails to your service provider so they can investigate and make sure others did not receive the same message and confirm its legitimacy.

STAGE 1 - Foundational Security

Step 7 Wireless

Overview

Wireless security is the prevention of unauthorized users from accessing your wireless network and stealing the data using your Wi-Fi network. To be precise, wireless security ensures protection to a Wi-Fi network from unauthorized access.

Why are they important?

Wireless networks introduce additional security risks. If you have a wireless network, make sure to take appropriate precautions to protect your information.

> *The majority (72%) of companies who suffered a data breach in the last year found that the network infiltration came from an unsecured wireless device, such as a printer, scanner, mobile phone or laptop connected to their Wi-Fi network (Probrand UK).*

Configuration

Wireless networks tend to be one of the more significant areas of risk that organizations neglect. Are you doing everything you should to make sure your wireless is configured securely? Here are the best practices you can follow to ensure your wireless is properly protected.

Essential	Better	Optimized
• Require an up to date wireless standard (e.g. WPA 3). • Do not share the wireless password with end users and change on a regular basis. • Do not allow personal / unmanaged devices on corporate wireless. • Require that all default passwords to your wireless router are changed during implementation. • Remote access for management console is disabled.	• Utilize a passwordless form of authentication. • Ensure proper wireless coverage. • Establish a guest network. • Ensure routers, modems, access points (APs) are kept up to date.	• Access points are strategically/ securely placed • Require separate VLANs for different types of devices or departments. • Rouge access points are monitored for.
To Do	**To Do**	**To Do**
□ Configure wireless networks to use a secure wireless standard like WPA3. Older standards, such as WPA and WEP, are no longer considered secure. □ Do not provide the wireless password to end-users or guests, unless you have a dedicated guest network that is logically	□ Utilize a better form of authentication besides just a pre-shared key (PSK). This could be certificate based, unique user ID and password for all, or RADIUS server. □ Ensure wireless signals do not broadcast outside of necessary areas.	□ Physically secure access points as best as possible in order to prevent tampering or theft. This can be done by placing them high on ceilings or behind a locked door. □ Utilize VLANs for different types of devices (e.g. corporate laptops, IoT, medical equipment, etc.) or different departments (e.g. finance, human resources,

separated from your corporate network.

- ☐ Setup a schedule to periodically change wireless password.
- ☐ Remove any personal or unmanaged devices from corporate network. Do not allow personal devices or unmanaged device to connect to your corporate wireless network.
- ☐ Ensure all default passwords are changed on wireless equipment.
- ☐ Disable any externally accessible remote management consoles for the wireless network.
- ☐ Setup a guest network for personal devices that is separate from internal network.
- ☐ Establish standard operating procedures to ensure network/ wireless equipment are updated on a regular basis.

etc.) to provide separation of network traffic.

- ☐ Monitor for rogue access points and remove any that are found.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning wireless security. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Do employees have access or the ability to add devices to the corporate wireless network?	Either the managed service provider needs to add all devices to wireless or a very limited number of people within your organization can add devices to corporate wireless.	Everyone knows the corporate wireless password and puts their personal phones and devices on the same wireless network.	If a wireless network is setup that utilizes a shared password that everyone knows, users can place on the network any type of device that could be infected or vulnerable to attack.
Do you provide any type of monitoring of the wireless network to ensure non-managed devices aren't connected?	MSP receive alerts when a new device is added to a corporate wireless network and can follow up to ensure its legitimacy.	No active monitoring or periodic review of devices connected to corporate wireless.	Unmanaged or improperly configured devices on a corporate network can provide an entry point for cybercriminals. Ensuring devices like a thermostat or piece of equipment isn't randomly placed on the corporate wireless can significantly reduce your cyber risk.
Can I access internal resources from the guest network?	You can't access internal resources (e.g. file server, internal applications) from the wireless without a VPN or another type of remote service.	You can access internal resources on the guest network. If you can access the resources so can anyone else on the wireless network.	Proper segmentation between guest and corporate wireless is essential, especially if users outside of your organization have access to the guest network.

STAGE 1 - Foundational Security

Step 8 Password Management

Overview

Passwords are a string of characters used for authenticating a user to a computer, system, or service. Although passwords remain one of the most common methods of authentication available, they are subjected to several security threats when mishandled. Password management is a set of principles and best practices to be enforced by the system or followed by users while creating, storing, and efficiently managing password to secure passwords and prevent unauthorized access.

Why are they important?

Password managers take the hassle out of creating and remembering strong passwords. It's that simple. Passwords are stolen all the time. Sites and services are at risk of breaches as much as you are to phishing attacks that try to trick you into turning over your password.

Configuration

Nobody likes passwords, but they're a fact of life. Are you doing everything you should to make sure users within your organization create and manage their passwords securely? Here are the best practices you can follow to ensure proper password management throughout your organization.

Essential	Better	Optimized
• Utilize a service or tool to securely store passwords. • Require a minimum of 8-character passwords. • Require passwords to require complexity (e.g. uppercase, special character, number, etc.). • Require lockout after 5 failed login attempts. • Do not allow reuse of passwords.	• Utilize a service or tool to securely store passwords with multi-factor authentication enabled. • Established procedures for shared credentials or service accounts. • Require a minimum of 12-character passwords. • Password education provided to all users.	• Utilize a centrally managed service or tool to securely store passwords for the organization. • Require a minimum of 15-character passwords. • Utilize of passphrases. • Utilize a blocklist of known compromised passwords.
To Do	**To Do**	**To Do**
□ Implement a tool to allow users to manage their passwords (e.g. LastPass, 1Password, KeePass). □ Set a minimum password length for all password to 8 characters. □ Enabled complexity for password requirements (e.g. uppercase, special character, number, etc.). □ Configure accounts to lock after 5 failed login attempts.	□ Implement a tool or service that allows users to manage their passwords with multifactor authentication required to access stored passwords. □ Implement a tool or service that allows users to securely share passwords when required (e.g. IT service accounts). □ Set a minimum password length for all password to 12 characters.	□ Implement a tool or service that allows users to manage their passwords that is centrally managed by the organization. □ Set a minimum password length for all password to 15 characters. □ Allow users to use passphrases (20+ characters while removing complexity requirements). □ Utilize a list of known compromised or common passwords that can't be used for organizational resources.

☐ Configure a password history of 7 so users can't reset password to the same password.	☐ Educate users on password best practice (not to reuse passwords, not to share, etc.).	

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning password management. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Does your service provide us with access to a password manager?	MSP provide access to a secure password manager as part of their service.	They don't offer a password manager and don't even have an option to add the service on for an additional fee.	Not providing users access to a password manager leads to users reusing passwords, writing them down, or using easily guessed passwords. This can lead to account compromises and data breaches.
What is your internal password policy?	15+ character passwords and passphrases, utilize a tool or service to ensure known bad passwords are not used by employees.	6-character passwords, that never expire.	When it comes to the length of passwords, longer is always better, and the reuse of passwords leads to credential stuffing. This can lead to account compromises and data breaches.

STAGE 2 - Policies & Awareness

Step 1 Email Phishing Exercises

Overview

Phishing is a type of online scam where criminals impersonate legitimate organizations via email, text message, advertisement or other means in order to steal sensitive information. Email phishing exercises are simulated phishing emails used to test and educate users. The emails within these exercises can spoof internal personnel, ask for sensitive information, or trick a user into entering their credentials into a phony login.

Why are they important?

Actual testing and experience are one of the best ways to inform users of the threat of phishing.

> *Ninety five percent (95%) of all attacks on enterprise networks are the result of a successful phishing attack (SANS Institute)*

Configuration

Live action testing is one of the best training mechanisms. Are you doing everything you should to make sure users within your organization are properly trained to spot and report phishing? Here are the best practices you can follow to provide email phishing to your organization.

Essential	Better	Optimized
• Conduct quarterly simulated phishing emails for all users.	• Conduct bi-monthly phishing for all users.	• Conduct monthly phishing for all users.

	• Develop a baseline, monitor and track phishing assessment results. • Utilize personalized simulated emails.	• Share the results of phishing assessments with leadership. • Establish spearphishing (i.e., targeted) assessments for high risk users. • Conduct vishing (voice phishing) and smishing (text message phishing) assessments.
To Do	**To Do**	**To Do**
□ Obtain buy in from leadership on ongoing simulated phishing assessments. □ Perform quarterly phishing assessments for all users. □ Provide additional training to users who fail a simulated phishing test.	□ Perform bi-monthly phishing assessments for all users. □ Develop a baseline for click rate of all users, then monitor and track ongoing phishing assessments comparing to the baseline. □ Determine high click individuals or departments and provide additional education. □ Develop personalized phishing emails to simulate realistic attempts.	□ Conduct monthly phishing assessments for all users. □ Present results to leadership regularly. □ Conduct spearphishing assessments on high risk individuals (e.g. CEO, CFO, IT leadership, individuals who have access to large amounts of data). □ Conduct periodic vishing or smishing assessments on a subset of users.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning simulated phishing emails. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Do you offer phishing as a service or is it part of your offering?	Monthly phishing is part of your contract with your MSP or they offer it as an additional service.	MSP does not offer phishing as service.	Simulated phishing is one of the best educations you can offer to end users. Without proper testing and education, how do you expect users to spot or report phishing emails.
Do you send simulated phishing to users internally to your organization (the MSP employees)?	MSP perform periodic phishing assessments to all their employees.	MSP does not perform phishing on their own employees.	MSPs are one of the largest targets for criminals and they utilize phishing to get inside of these organizations. Without proper testing and education, the MSP is not protecting their company from an attack which in turn could affect your organization.

STAGE 2 - Policies & Awareness

Step 2 Security Awareness Training

Overview

A comprehensive security awareness program sets clear cybersecurity expectations for all employees and educates users on how to recognize attack vectors, help prevent cyber-related incidents and respond to potential threats. Training employees about safe online computing, strong passwords, social engineering and more will help mold individuals into your first line of cyber defense and ensure the confidentiality of sensitive business data.

Why are they important?

It is said that the “human” is the weakest link in any organization’s security posture. Without an embedded culture of cybersecurity awareness and enforcement, all those fancy and expensive systems aren’t going to do you much good.

> *Fifty three percent (53%) of people admit they use the same password for work and personal accounts. (Security Magazine)*

Configuration

End users can be the last and sometimes the only defense against cyber-attacks. Are you doing everything you should to make sure users within your organization are properly educated on potential threats and best practices? Here are the best practices for security awareness training.

Essential	Better	Optimized
• Require awareness training for all new hires. • Require annual awareness training for all users.	• Require ongoing security awareness training throughout the year for all users.	• Require role-based training. • Establish live/ real world training. • Create a cyber conscience culture.
To Do	**To Do**	**To Do**
□ Obtain buy in from leadership on security awareness training. □ Provide security awareness training for users upon hiring. □ Provide annual awareness training for all users.	□ Provide ongoing security awareness training for all users. □ Provide monthly updates, videos, quizzes, or presentation on cyber topics and threats. □ Provide educational material relatable and useful outside of work (e.g. personal account management).	□ Provide role-based training for users in specific roles (e.g. data owners, executive leadership, customer service). □ Conduct in person social engineering assessments (shoulder surfing, piggybacking, dumpster diving, USB drops, etc.). □ Create a culture of reinforcement and motivation for constant vigilance about cybersecurity.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning security awareness training. We’ve also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact

Do you offer security awareness training and ongoing education for all users within our organization?	Security awareness training is part of your contract with your MSP or they offer it as an additional service.	MSP does not offer security awareness training.	Without proper security awareness training, you are relying on employees to know about the most recent cyber-attacks and how to report them. Ongoing security awareness training is crucial for all employees as they are sometimes the last layer of defense against attack.
Do you provide security awareness training to all users internally to your organization (the MSP employees)?	MSP provides security awareness training to all their employees.	MSP does not provide security awareness training for all its employees.	MSPs are one of the largest targets for criminals. Without proper education, the MSP is not protecting their company from an attack which in turn could affect your organization.
How do you ensure your employees stay current on all the cyber-attacks/ techniques used by criminals?	MSP ensures employees go to yearly educational seminars or classes to learn about the latest cyber threats and techniques to prevent them.	MSP does not provide opportunities for employees to attend trainings on the latest cyber-attacks and techniques.	If MSPs do not continually mature their practices and employees, they could fall behind in the latest types of cyber-attacks and are much more likely to be involved in an incident.

STAGE 2 - Policies & Awareness

Step 3 Acceptable Use Policy

Overview

An Acceptable Use Policy (AUP) is an important document which governs the use of the company resources and covers a wide range of issues surrounding the rights, responsibilities and privileges – as well as sanctions – connected with computer use. An AUP clearly states what the user is and is not allowed to do with these resources.

Why are they important?

An Acceptable Use Policy is an important document that can demonstrate due diligence with regards to the security of an organization. It also provides users easily digestible content on the do's and don'ts of the organization.

Configuration

Are you educating end users what is acceptable and not while at work? Here are the best practices for an acceptable use policy.

Essential	Better	Optimized
• Establish an AUP. • Require all users to sign an AUP upon hire. • Ensure the AUP is easily accessible/ understandable to all users.	• Require all users to sign the AUP on an annual basis. • Require the AUP to be reviewed and updated annually by leadership.	• Provide periodic reminders to all users on acceptable/ unacceptable actions. • Solicit feedback from end users.
To Do	**To Do**	**To Do**

- □ Develop an AUP with leadership buy in.
- □ Assign responsibility for tracking and monitoring AUP signing by all users.
- □ The AUP should outline activities that are or are not acceptable concerning IT resources or company data.
- □ Have all users sign AUP during the hiring process.
- □ Ensure the AUP is easily accessible for all users.
- □ Ensure the AUP is easily understandable by all users (avoid lawyer speak).
- □ Have all users sign the acceptable use policy every twelve months or any time the AUP is updated.
- □ Ensure the AUP is reviewed and updated annually by leadership to ensure topics are relevant.
- □ Educate users on specific topics within the AUP on a periodic basis to ensure they understand and follow the AUP.
- □ Incorporate the AUP into the welcome screen when logging onto a company resource.
- □ As part of the annual review process, solicit and incorporate end user feedback into the AUP.

Managed Service Provider (MSP) Questions

Outsource your IT? Remember that a resource like an Acceptable Use Policy is probably not something they will provide you and it's up to you to develop and provide to your employees. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Does your organization have an acceptable use policy that is reviewed and signed by all employees?	MSP has an acceptable use policy that is shared with all of their employees.	MSP does not have an acceptable use policy.	An acceptable use policy is an important document that can demonstrate that an organization educates its users on the do's and don'ts the organization's security practices. If an MSP doesn't utilize an acceptable use policy, they might not be doing everything they should to ensure employees are properly educated.

STAGE 2 - Policies & Awareness

Step 4 Cybersecurity Policies

Overview

A cybersecurity policy sets the standards of behavior for activities such as the encryption of email attachments and restrictions on the use of social media.

Why are they important?

Cybersecurity policies are important because cyberattacks and data breaches are potentially costly. At the same time, employees are often the weakest links in an organization's security. Without proper guidance and standards, the organization is susceptible to cyber-attacks and lawsuits.

Configuration

Do you provide guidance and standards to end users on things like password requirements, being able to share data, and if they can install software? Formal documented cybersecurity policies provide guidance and consistency for all users within an organization. Here are the best practices for creating cybersecurity policies.

Essential	Better	Optimized
• Establish a high-level cybersecurity policy. • Obtain buy in from leadership.	• Establish a cybersecurity policy. • Require policies to be reviewed and updated annually. • Require policies to be easily accessible by all staff. • Policies outline roles and responsibilities for all users.	• Encompassing cybersecurity policy for all areas. • Cybersecurity policy is a living document.
To Do	**To Do**	**To Do**
□ Develop a cybersecurity policy with leadership buy in. □ Establish policies for standards and guidelines on specific controls including (access control, audit and logging, contingency planning, incident response, network administration, physical and environmental protections, security awareness, system operations, and vendor management).	□ Establish policies for standards and guidelines on specific controls including (asset management, change control, data retention, configuration management, encryption, remote access, removable media, vulnerability management) □ Establish a review process to review policies on an annual basis. □ Ensure policies are easily accessible to all staff for easy reference. □ Ensure policies outline roles and responsibilities for specific users (e.g. leadership, IT, end users, etc.).	□ Establish policies for standards and guidelines on specific controls including (BYOD, Data Classification, software development, software lifecycle, risk management, IT strategy/ planning) □ Regularly update and change policies as compliance, business, and technology change.

Managed Service Provider (MSP) Questions

Outsource your IT? Remember that a resource like a Cybersecurity Policy is probably not something they will provide you and it's up to you to develop and provide to your employees. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Does your organization have cybersecurity policies?	MSP have formal documented cybersecurity policies that outline controls like access control, audit and logging,	MSP does not maintain formal documented cybersecurity policies	If an MSP does not have formal documented cybersecurity policies, they are likely inconsistent with system configurations and settings and security practices, which can lead to incidents or a breach.

	contingency planning, incident response, network administration, physical and environmental protections, security awareness, system operations, and vendor management.		

STAGE 3 - Key Processes

Step 1 Asset Management

Overview

IT asset management is the process of ensuring an organization's assets are accounted for, deployed, maintained, upgraded, and disposed of when the time comes. Put simply, it's making sure that the valuable items, tangible and intangible, in your organization are tracked and being used.

Why are they important?

You can't protect what you don't know you have. Without a proper inventory of assets, data can be lost, stolen, mishandled, or disposed of improperly. All of which can lead to a major gap in an organization cybersecurity program.

Eighty percent (*80%) of workers admit to using SaaS applications at work without getting approval from IT. (McAfee)*

Configuration

Do you know where all your organization's assets reside? If pressed would you be able to locate a specific device quickly? Does your organization know all online services your organization is currently utilizing? Here are the best practices you can follow to manage the assets within your organization.

Essential	Better	Optimized
• Maintain a manual inventory of all endpoints. • Establish a process for onboarding and disposal of hardware. • Utilize a secure disposable procedure.	• Utilize a tool or service for asset tracking. • Maintain an inventory of all hardware devices. • Maintain and inventory of all installed software. • Require disposal certificate.	• Maintain an inventory of all Software as a Service (SaaS). • Active scanning for new devices. • Conduct periodic audits of software and hardware.
To Do	**To Do**	**To Do**
□ Utilize a tool or spreadsheet to inventory endpoints (workstations, laptops, tablets, phones). □ Ensure inventory elements include asset types, serial	□ Utilize a tool to inventory all IT assets (e.g. endpoints, servers, network equipment, printers, storage devices, etc.).	□ Utilize a tool or spreadsheet to inventory all software as a service (SaaS). □ Perform regular scanning of the network to identify new or unmanaged devices.

numbers, purchase price, owner, warranty information, and location. ☐ Establish a procedure for onboarding new IT equipment to ensure its properly tracked. ☐ Establish a procedure for removing IT equipment from inventory system when retiring or disposing. ☐ Establish a secure disposable procedure from IT equipment that store information (e.g. hard drives, USB storage, printers, etc.). Third-party services offer this service at a relatively low cost.	☐ Track or utilize a tool to maintain an inventory of all installed software within the organization. ☐ Establish a procedure for installing and maintaining software. ☐ Require a certificate of destruction for all device or media that stores/ process data.	☐ Perform regular audits of hardware to ensure devices are not lost or stolen. ☐ Perform regular audits of installed software to ensure licenses are properly managed and non-approved applications are not installed. ☐ Perform regular audits of internet traffic to ensure all Software as a Service (SaaS's) are accounted for.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning asset management. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Do you keep an inventory of all our devices?	MSP keeps an up to date inventory of all your devices and is alerted when a new device is installed or connected to the network.	MSP doesn't keep an up to date inventory and would not be aware if a new device was added to the network.	Without a proper inventory of devices, an MSP can't provide assurance that all preventative controls are being applied to devices which could leave your organization vulnerable.
Can you run a report to see what applications are installed on endpoints?	MSP can provide a report of all installed applications on endpoints.	MSP can't quickly generate a report of installed applications.	Ensuring that only approved and managed applications are installed on endpoints is essential to an organization. Unapproved, pirated, unsupported software can introduce vulnerabilities to the organizations.
Can you monitor web traffic for unauthorized SaaS?	MSP can actively monitor and/or block unauthorized SaaS (e.g. file storage like DropBox).	MSP can't monitor for unauthorized SaaS.	If an organization can't see all the online services (SaaS) employees utilize, it can't properly protect those services.

STAGE 3 - Key Processes

Step 2 Patch Management

Overview

Patch management is the process of distributing and applying updates to software, operating systems, and hardware. These patches are often necessary to correct errors (also referred to as "vulnerabilities" or "bugs").

Why are they important?

Software vulnerabilities or bugs are exploited by hackers to access individual systems—and from there, your broader network and data. Applying a patch as quickly as possible reduces the chances attackers must access your systems. In addition, for compliance reasons, particularly when it comes to health information, financial information, or other personal data, you need to have good patch management procedures in place.

Fifty seven percent (57%) of data breaches are attributed to poor patch management. (Ponemon)

Configuration

Do you know how often updates are applied to your organization's devices? Are you aware of any unsupported systems, applications, or hardware? Here are the best practices you can follow to manage updates and patches within your organization.

Essential	Better	Optimized
• Monthly updates are applied to critical and externally facing systems. • Sign up to receive notifications from vendors concerning patches and updates. • Do not allow end of life (EOL) devices or software within the environment.	• Utilize a software update tool or service to manage patches and security updates. • Ensure all operating systems and applications updates/ patches are automated. • Updates are reviewed and tested before deployment.	• Establish a formal patching/ update process for all devices and applications (3rd party applications, IoT devices, network equipment, firmware, bios, etc.). • Report to leadership on progress/ status of patch management process. • Establish a formal exception process for systems or devices that are unable to receive updates in a timely manner.
To Do	**To Do**	**To Do**
☐ Apply all security updates and patches to critical systems within the organization as soon as possible. ☐ Apply all security updates and patches to systems that are externally facing as soon as possible. ☐ Sign up to receive notifications from vendors concerning security updates and patches. ☐ Ensure that devices, software, and operating systems are all still	☐ Utilize a tool or service to apply updates to all servers and workstations monthly. ☐ Establish automated processes for updating/ patching operating systems and applications. ☐ Establish a sample of endpoints and servers to test patches/ updates before pushing out to all devices.	☐ Establish a formal patching/ update process for all nonstandard devices (IoT devices, network equipment, medical equipment, machinery, etc.). ☐ Establish a formal patching/ update process for all 3rd party applications (e.g. java, adobe reader, etc.). ☐ Keep management up to date on patch management progress, especially when some systems

supported and can receive updates/ patches. Avoid using software that is no longer supported by the vendor (e.g., Windows XP, Windows 7, Windows Server 2008 etc.)	☐ Establish a development environment to test software patches for critical applications.	are not updated or no longer supported. ☐ Establish a formal exception process for systems that can't be updated in a timely manner. This process should include a risk analysis.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning patch management. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Do you apply security updates/ patches on a regular basis to our devices?	MSP applies updates within a few weeks of their release.	MSP only applies updates on a quarterly basis.	If systems are not updated/ patched in a timely manner it leaves the organization vulnerable to attack. Patching ensures that known security vulnerabilities are closed before they can be exploited by criminals.
Do you apply updates/ manage non-Window devices (e.g. Mac, iOS, Android)?	MSP manages and applies updates across multiple operating systems.	MSP only manages and updates Window devices.	Many organizations have multiple operating systems running and they all need to receive patches and updates to ensure the organization is protected from attack.
Can you provide a report that shows all our devices are up to date with the latest security patches?	MSP provides regular reports that show all of your organization's devices and that the latest patches have been applied.	MSP can't provide evidence that devices are up to date.	As part of your due diligence, you should ensure that your provider is applying updates on a regular basis. If they can't provide this evidence, how can you be assured updates are being applied.

STAGE 3 - Key Processes

Step 3 Securing Remote Workers

Overview

Remote workers present a unique challenge for organizations because remote work environments don't usually have the same safeguards as an office. When an employee is at the office, they are working behind layers of preventive security controls. Ensuring remote workers are properly protected outside of the organization is essential for protecting an organization's data and systems.

Why are they important?

When computers leave the perimeter of the office network, new risks arise. With the sudden push to remote work, organizations are left wondering if they have sufficient security to protect remote workers. Without proper security configurations for remote workers, organizations are increasing their risk.

In a recent Malwarebytes report, 44% of organization said they didn't provide cybersecurity training focused on the potential threats of working from home, and 45% didn't analyze the security or privacy features in the software tools considered necessary for remote working.

Configuration

Are you doing everything you should to make sure endpoints are properly configured for remote work and users are properly educated on working from home? Here are the best practices for securing remote workers.

Essential	Better	Optimized
• Require all employees to sign an acceptable use policy for working remotely. • Utilize a full tunnel VPN. • Require multi-factor authentication. • Utilize an endpoint detection tool on remote devices.	• Educate users on working remotely and securing home. • Require application and system updates to be automatically pushed to remote devices. • Require endpoints to be encrypted. • Ensure the endpoint detection tool reports findings without VPN connectivity.	• Endpoints are configured with remote wipe capability. • Provide IT remote access capabilities to remote workers.
To Do	**To Do**	**To Do**
□ Establish an acceptable use policy for working remotely and require that all users sign. □ Ensure that users have a secure method to access company resources (e.g. VPN). □ Ensure VPN connections are full tunnel, so all traffic is properly being monitored. □ Ensure VPN access requires multi-factor authentication. □ Ensure all remote workers have an endpoint detection tool installed on their device. □ Ensure endpoint detection tool functions without VPN access to corporate network.	□ Provide education for securing home network and work area for all remote users. □ Provide education for securing devices when traveling. □ Ensure security patches and updates are still applied to devices when not connected to corporate network. □ Establish policies to require all devices to be configured with full disk encryption. This includes mobile device, laptops, and workstations. □ Ensure the endpoint detection tool can alert IT of events even when not connected to corporate network.	□ Establish a procedure to remotely wipe a device in the event they are lost or stolen. □ Ensure IT has remote access capabilities to remote into devices even when not connected to corporate network.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning securing remote workers. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Do we have a way to work remotely? Can	MSP provides a VPN or another type of secure	MSP cannot provide a secure solution to	If your organization doesn't have a secure way to access internal resources

we securely access internal resources from outside our network?	solution to work remotely and access internal resources when needed.	access internal resources.	remotely or while traveling, it can't securely connect over untrusted Wi-Fi or internet connection. This could result in leaving your organization vulnerable to attack or impairing your ability to work.
Are all our devices encrypted in the event a device is lost or stolen?	MSP configures all your endpoints with full disk encryption enabled.	MSP does not enable encryption on endpoints.	If a device is lost or stolen and it is encrypted, it provides some assurance that any data residing on it will not be retrievable. If a device is lost or stolen and it's not encrypted the data is easily accessible.
Is our monitoring ability decreased if workers are remote (e.g. website still filtered, events like a virus still trigger an alert)?	MSP configures devices so that if it is connected to the internet they can monitor and configure systems.	MSP cannot monitor, update, or provide support if the device is not connected to the corporate network.	Without the ability to monitor, update, and provide support to remote workers, employees could circumvent security controls. This could lead to devices being outdated, data residing outside of managed services, or inability to perform their job.

STAGE 3 - Key Processes

Step 4 Mobile Device Management (MDM)

Overview

Mobile device management (MDM) is a security software that enables organizations to implement policies that secure, monitor, and manage end-user mobile devices. MDM helps ensure the security of a corporate network while allowing users to use their own devices and work more efficiently.

Why are they important?

MDM keeps your organization's data protected and ensures you retain control over confidential information. If a mobile device is lost or stolen, MDM solutions can remotely lock and wipe all data. Remote locking and wiping capabilities enable companies to keep devices and data secure.

Configuration

Do you allow users to access corporate email on their personal devices? What if that device was lost or stolen do you know if any confidential data resided on it? Here are the best practices you can follow to ensure mobile devices are protected.

Essential	Better	Optimized
• Develop or utilize a mobile device policy. • Require a tool or service for the administration of mobile devices. • Develop an enrollment process for all mobile devices. • Require a PIN or Passcode for devices that have access to corporate data/ resources.	• Mobile devices are configured with remote wipe. • Mobile devices isolate work apps from personal on personal devices. • Require an inactivity lock to be enabled.	• Prevent data from being downloaded locally to mobile devices. • Limit the types of mobile applications that can be downloaded onto mobile devices. • Erase data after 10 failed login attempts.

• Require full disk encryption.		
To Do	**To Do**	**To Do**
☐ Establish a mobile device policy that outlines whether personal devices will be permitted to access corporate data. ☐ Utilize a tool or service to administer mobile devices, this includes ensuring phones are updated, not rooted, etc. ☐ Establish an enrollment process for all mobile devices to ensure they are properly configured and managed. ☐ Ensure that all devices are secured with a PIN or passcode. ☐ Ensure that all device have full disk encryption enabled.	☐ Ensure a tool or service can remotely wipe a mobile device in the event it is lost or stolen. ☐ Incorporate isolation of work applications from personal devices on personally owned devices. ☐ Enabled automatic locking of a device after 2 minutes of inactivity.	☐ Ensure that data can't be downloaded locally to mobile devices from corporate resources (e.g. email, online storage, etc.). ☐ Configure mobile device not to be allowed to install malicious, unapproved mobile apps. ☐ Configure devices to automatically wipe data after 10 consecutive failed login attempts.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning mobile device management. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Does your service include managing mobile devices, including personal devices that access corporate resources?	MSP has a tool (e.g. Microsoft Intune) that they can be used to manage mobile device (even personal devices).	MSP doesn't offer mobile device management.	Nearly all users have corporate email or access to other services (e.g. OneDrive) on their personal devices. Proper controls are needed to ensure devices are properly configured and able to be wiped. This ensures corporate data is protected.

STAGE 3 - Key Processes

Step 5 Standard Configuration

Overview

Standardized configurations, or baselines, are a document or method that describe how a device should be configured. These baselines indicate the specifications of information system components (hardware, firmware, and software).

Why are they important?

Attackers are looking for systems that have settings that are immediately vulnerable. Once an attacker exploits a system, they start making changes. By setting a gold standard configuration for your systems and continuously monitoring for indicators of compromise, organizations can stop or quickly identify a breach.

Configuration

Consistency is key. It's easier to identify issues and apply updates when systems utilize the same standards during build and deployment. Here are the best practices you can follow to ensure your organization have standard configurations.

Essential	Better	Optimized
• Utilize a standard configuration for endpoints and servers. • Limit access to change standard configurations.	• Utilize a standard configuration for network devices, mobile devices, printers, and scanners. • Require a review process for changes to standard configurations. • Establish an exception process for devices that can't follow standard configurations.	• Require system hardening be incorporated into standard configuration. • Conduct security impact analysis for changes to standard configurations. • Require least functionality for configurations.
To Do	**To Do**	**To Do**
□ Establish standard configurations for endpoints (e.g. lockout policy, firewall/ encryption enabled, removal of bloatware/ games, backgrounds, etc.). □ Establish standard configurations for servers (e.g. disabling all unnecessary services, administrator password changes, guest account disabled, etc.). □ Ensure that changing standard configuration settings are limited to select individuals.	□ Establish standard configurations for networking equipment (firewalls, switches, routers, access points). □ Establish standard configurations for corporate owned mobile devices (iPads, tablets, smartphones). □ Establish standard configurations for printers and scanners, especially limiting the ability to store copies of scanned images. □ Develop a process that all changes to standard configurations must be reviewed and approved before changes are implemented. □ Establish a formal exception process, including an appropriate level of approval, for devices that can not follow standard configurations.	□ Establish standard configurations that are hardened to meet industry best practices for security, this can be accomplished using tools and techniques. □ As part of the change process for standard configuration, incorporate a security impact analysis to determine any protentional risks with the changes. □ Ensure that all configurations factor in the principle of least functionality, to ensure only necessary services or settings are configured for a system to perform its duty.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning standard configurations. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Are all our systems configured using a standard configuration? Are	All systems (endpoints, servers, network equipment) utilize standard	Systems are configured with default (out of the box) settings.	Standard configuration makes updates and patching significantly easier and provides consistency for configuration and settings. If each system is

systems configured to follow the principle of least functionality?	configurations that follow the principle of least functionality.		configured differently it's much more difficult to determine if a system is configured correctly. System defaults tend not to be the most secure and deploying systems with defaults may result in insufficient security controls.
Are our systems configured utilizing a hardened standard like CIS benchmarks?	All systems are configured utilizing a hardened standard like CIS.	Systems are configured with default (out of the box) settings.	CIS benchmarks or other hardening standards provide best practices for configuring systems. Without proper attention to secure configurations system could become vulnerable to attack.

STAGE 3 - Key Processes

Step 6 Vulnerability Scanning

Overview

Vulnerability scanning utilizes automated tools that allow organizations to check if their networks, systems and applications have security weaknesses that could expose them to attacks.

Why are they important?

Vulnerabilities scans identify security gaps that could be abused by attackers to damage network assets, trigger a denial of service, and/or steal potentially sensitive information. Scanning for and remediating identified risks can greatly decrease the likelihood of an incident.

Configuration

How do you know your organization's patch management system didn't miss something? Do you know if your website has been properly configured? Here are the best practices you can follow for vulnerability scans.

Essential	Better	Optimized
• Require all externally facing resources be scanned on a quarterly basis. • Develop vulnerability thresholds and remediation plans.	• Require all externally facing resources be scanned on a monthly basis. • Require critical or essential internal resources to be scanned quarterly. • Track and manage vulnerabilities.	• Require all externally facing resources be scanned on a weekly basis. • Require all internal resources scanned monthly. • Report findings and remediation progress to leadership. • Require a penetration test to be performed annually. • Require periodic sensitive data scans.
To Do	**To Do**	**To Do**
□ Perform or utilize a service to scan all externally facing resources quarterly to detect any	□ Perform or utilize a service to scan all externally facing resources monthly to detect any	□ Perform or utilize a service to scan all externally facing resources weekly to detect any

potential vulnerabilities and ensure proper configurations. ☐ Establish vulnerability thresholds and remediation plans for found vulnerabilities by criticality (e.g. High risk = remediate within 3 days, Low risk = potential accept the risk).	protentional vulnerabilities and ensure proper configurations. ☐ Perform or utilize a service to scan all critical internally housed resources quarterly to detect any protentional vulnerabilities and ensure proper configurations. ☐ Utilize a tool or integrate scanning tool with a ticketing system to track and monitor found vulnerabilities and track remediation.	protentional vulnerabilities and ensure proper configurations. ☐ Perform or utilize a service to scan all critical internally housed resources monthly to detect any protentional vulnerabilities and ensure proper configurations. ☐ Ensure leadership is provided updates on findings and remediation status. ☐ Have a third party perform a penetration test annually to identify any gaps that could be exploited by criminals. ☐ Perform periodic sensitive data scans on file servers, endpoints to ensure sensitive data such as SSN, credit cards, are not being stored outside of approved repositories.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning Vulnerability Scanning. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Do you perform vulnerability scans on any of our internal or external systems?	MSP perform regular vulnerability scans of your internal and external systems and provides you with a report of findings and their remediation plan.	MSP does not perform any type of vulnerability scanning on your systems.	Performing regular vulnerability scans ensure patch management and standard configurations are followed. Without vulnerability scans, systems may become misconfigured and go noticed until an incident occurs.
Do you perform regular vulnerability scans on your own internal systems?	MSP performs regular vulnerability scans on their own systems to ensure they are properly configured and maintained.	MSP does not perform regular vulnerability scans on their own systems.	If an MSP doesn't perform regular vulnerability scans on their networks, they cannot ensure all of their systems are properly configured to protect your data is protected.

STAGE 4 - Incident Preparedness

Step 1 Incident Response (IR) Planning

Overview

An incident response plan ensures that in the event of a security breach, the right personnel and procedures are in place to effectively deal with a threat. Having an incident response plan in place ensures that a structured investigation can take place to provide a targeted response to contain and remediate the threat.

Why are they important?

The best time to prepare for an incident is before one happens. A business must have an incident response plan so that under the pressure of an incident the correct decisions can be made to bring the situation back under control.

> *A recent study by Cyentia Institute shows that companies that don't have a good cyber incident response plan suffered losses 2.8 times greater than their counterparts that did have a great cyber incident response plan.*

Configuration

Does your organization know how it would respond to a news agency reaching out asking about seeing private company information or customer data on the internet? Here are the best practices you can follow to ensure you are prepared for an incident.

Essential	Better	Optimized
• Essential contact information has been established for an incident response service provider, FBI, local law enforcement, cyber insurance company, legal counsel. • Develop an incident response plan. • Define an incident vs an event. • Define when notifications of the incident are required.	• Educate users concerning their roles and responsibilities. • Require event/ incident tracking. • Retain the services of an incident response provider.	• Utilize an incident response playbook. • Organization has the expertise to perform forensic analysis. • Utilize an incident response plan that outlines activities when an external vendor has an incident. • Require lessons learned after all incidents.
To Do	**To Do**	**To Do**
□ Document and maintain a list of contact information for an incident response service provider, FBI, local law enforcement, cyber insurance company, and legal counsel. □ Store essential contact information in multiple locations, including a hard copy. □ Periodically ensure contact information for contacts is still correct. □ Establish an incident response plan that outlines (scope, roles &	□ Ensure all users are educated on their roles and responsibilities concerning incident response. □ Establish a procedure to track events and incidents. □ Contract with an incident response provider to be ready to assist the organization in the event of a security incident.	□ Develop an incident response playbook for specific types of incidents (e.g. malware, phishing, ransomware, denial of service, etc.). □ Establish and train internal personnel to be able to forensically investigate an incident. □ Establish incident response plans, in the event a 3rd party suffers a breach that involves your organization's data.

responsibilities, definition of an incident, how to handle generic incidents, when to notify affected personnel).		□ As part of incident response plan, establish lessons learned and incorporate lessons into hardening systems, updating policies, establishing better incident response plans.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning incident response planning. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
If our organization has an incident, can you provide incident response support?	MSP has the resources or have partnered with an incident response service provider to handle incidents.	MSP cannot offer help in the event of an incident and has not engaged with an incident response service provider.	Having a team of professionals that specialize in incident response is necessary when dealing with most types of incidents. If you don't have access to professionals, it can greatly increase the cost and time of recovery.
Does the MSP have their own incident response plan?	MSP has a formal incident response plan.	MSP does not have a formal incidents response plan.	If your MSP has an incident it's more than likely going to affect your business. Without a formal plan in place, the recovery time for your MSP is greatly increased.

STAGE 4 - Incident Preparedness

Step 2 Incident Response Training & Testing

Overview

Incident response training involves educating all users of the organization. This training could include how to spot an incident, how to appropriately report an incident, or their role as a decision maker. The testing of the incident response plan is the process of determining if your organization's incident response plan has gaps or missing key personnel.

Why are they important?

Schools run tornado and fire drills, so everyone knows what to do and when. Incident response training and testing is the same premise. Training and testing employees on a regular basis prepare them for an actual event. The worst time to find out your incident response plan doesn't work is during a security incident.

Configuration

Does your organization educate users on how to report an incident? Does IT or leadership know how to react to a major incident? Here are the best practices you can follow to ensure you are prepared for an incident.

Essential	Better	Optimized
• Incident response training is provided to all users within the organization.	• Incident response team receives training on specific incident response techniques.	• Simulated "live" attacks are periodically performed.

	• Incident response tabletop exercises are conducted on a regular basis.	• Incident response plan is integrated with disaster recover/contingency plans.
To Do	**To Do**	**To Do**
☐ Establish training for all users on how to identify an incident and report an incident to appropriate personnel. This could be incorporated into the organization’s overall security awareness training.	☐ Establish training for incident response team members on investigation techniques, log collection, isolation, malware analysis, etc. ☐ Periodically perform incident response tabletop exercises with Leadership, IT, general counsel, HR, PR, and external incident response service provider.	☐ Periodically perform live simulated attacks to determine how users react to specific attacks. ☐ As part of incident response testing, ensure that plans integrate with disaster recovery/contingency plans to restore lost data or acquire new equipment.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning incident response training. We’ve also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Is your MSP willing to be included in incident response testing?	MSP initiates incident response training and testing or is willing to be part of your organization’s testing.	MSP does not provide incident response training or testing for your users and is not willing to be part of incident response testing.	Without proper education and testing, an organization cannot determine if their incident response plan will work or if there are any gaps within the plan.
Does the MSP regularly test their incident response plan?	MSP has a formal incident response plan that they regularly test.	MSP does not test its incident response plan.	If an MSP doesn’t test their own internal incident response plan, it could impact your organization in the event of an actual incident.

STAGE 5 - Security Monitoring

Step 1 Security Information & Event Management (SIEM) Solution

Overview

Security information and event management (SIEM) software gives organization both insight into and a track record of the activities within their IT environment. SIEM combined security event management (SEM) – which analyzes log and event data in real time to provide threat monitoring, event correlation and incident response – with security information management (SIM) which collects, analyzes and reports on log data. In essence, SIEM is a management layer above a firm’s existing systems and security controls that provides a broad yet comprehensive way to view and analyze all of a company’s network activity from a single interface.

Why are they important?

A key advantage to a SIEM is that the organization can spend their time watching for security threats in real time, rather than devoting their days to studying the inner workings of every single security product in their systems.

Configuration

If you suffer a cybersecurity breach you want to know how the breach happened. Here are the best practices for a log aggregation/ SIEM solution.

Essential	Better	Optimized
• Utilize basic log repository for critical or essential applications and systems. • Logs are properly managed and backed up.	• Utilize a tool or service to store and aggregate logs. • Require logs be ingested from intrusion detection systems, endpoint security, VPN concentrators, web filters, firewalls, domain controllers, etc. • Utilize alerts for anomalies. • Require minimal log retention.	• Perform testing of SIEM alerting. • Require logs be ingested from hosted solutions, routers, switches, application servers, database servers, wireless, vulnerability reports, etc. • Integrate threat intelligence into SIEM.
To Do	**To Do**	**To Do**
□ Establish a procedure for log storage for critical applications and systems (e.g. firewall, domain controllers, etc.). □ Ensure logs are routinely saved and backed up.	□ Utilize a tool or service to store and aggregate logs from key systems. □ Import logs from intrusion detection systems, servers, domain controllers, endpoint detection tools, web filters, firewalls, and VPN concentrators into tool or service. □ Setup alerts within SIEM for specific anomalies (e.g. large number of failed logins, unusual login location, failed 2FA, escalation of privileges, etc.). □ Establish a log retention procedure to ensure sufficient logs are kept (minimum of 2 months).	□ Periodically test SIEM alerts to ensure they are properly configured by triggering them with real world attacks. □ Expand log importation to include hosted solutions, routers, switches, application servers, database servers, wireless, vulnerability reports, etc. □ Integrate SIEM with threat intelligence services to prioritize alerts.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning a SIEM solution. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Are our logs being imported into a SIEM solution?	All critical logs are being sent and stored within a SIEM solution that has alerting and is monitored.	Logs are not being sent to a SIEM solution and rely on each individual system or application for log retention.	Log correlation and alerting is key to identifying an incident quickly. The quicker an incident is identified, the quicker it can be contained and irradiated.

STAGE 5 - Security Monitoring

Step 2 24 X 7 Security Operation Center (SOC) & Threat Hunting

Overview

A security operations center (SOC) is a facility that houses an information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The SOC team's goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes.

Threat hunting is the human-driven, proactive and iterative search through networks, endpoints, or datasets in order to detect malicious, suspicious, or risky activities that have evaded detection by existing automated tools.

There are third-party services providers who specialize in providing outsourced SOC and threat hunting services. For most organizations, the resources to conduct these activities are beyond their means to maintain, and they opt to outsources these services.

Why are they important?

24/7 monitoring provided by a SOC gives organizations an advantage to defend against incidents and intrusions, regardless of source, time of day, or attack type.

Configuration

Ideally, 24/7 monitoring of systems is established to ensure that any events can be quickly acted on. Here are the best practices for a 24/7 SOC and threat hunting.

Essential	Better	Optimized
• 24/7 monitoring of security detection tools. • SOC is integrated into organizations incident response plan.	• Require all network traffic to be monitored. • Threats are prioritized on risk.	• Active threat hunting
To Do	**To Do**	**To Do**
☐ Ensure security detection tools are monitored 24/7/365. ☐ Ensure SOC is able to digest or review all detection tools logs. ☐ Establish procedures for incident response/ coordination with the incident response team.	☐ Ensure that even internal traffic (east/ west traffic is monitored). ☐ Establish procedures to ensure threats are prioritize based on risk.	☐ Establish procedures to actively look for suspicious activity utilizing Hypothesis-driven investigations.

Managed Service Provider (MSP) Questions

Outsource your IT? Below is a list of questions to ask your Managed Service Provider concerning a 24x7 SOC/ Threat Hunting. We've also included examples of what would constitute a *Good Response* from your MSP, the type of response that would be a *Warning Sign* of a potential security risk, and the *Impact* of not addressing that risk.

Question	Good Response	Warning Sign	Impact
Does your service include a 24/7 staffed Security Operation Center (SOC)?	MSP provides 24/7 monitoring of security tools and report potential incidents within a timely manner.	MSP doesn’t offer 24/7 monitoring of your security tools.	Without 24/7 monitoring, an event could happen Friday evening and not be noticed or acted on till Monday morning; providing criminals ample time to exfiltrate data or cause major harm.
Are your systems monitored by a 24/7 SOC?	The MSP internal resources are monitored by a 24/7 SOC.	MSP does not actively monitor its internal resources or have a service provider monitoring for them.	If an MSP does not actively monitor its systems and it sustains a major incident, it could in turn take down your organization’s IT systems.

Appendix A – MSP Questions

Attached to the PDF is the complete list of question to ask your managed service provider in an excel format that can easily be edited. Also included in the excel spreadsheet is a copy of the questions that can easily be sent to your MSP.

MSP_Questions.xlsx

Appendix B – Configuration Tables (Excel Format)

Attached to the PDF is the complete list of all configuration tables in an excel format.

Cyber_Configuration_Checklist.xlsx

Glossary

Terminology

- **BitLocker -** is a full volume encryption feature included with Microsoft Windows operating system. It is designed to protect data by providing encryption for entire volumes. By default, it uses the AES encryption algorithm in cipher block chaining or XTS mode with a 128-bit or 256-bit key.
- **Data Loss Prevention (DLP) -** detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in use, in motion, and at rest
- **Data Retention -** defines the policies of persistent data and records management for meeting legal and business data archival requirements.
- **Domain Administrator** - in Windows is a user account that can edit information in Active Directory. It can modify the configuration of Active Directory servers and can modify any content stored in Active Directory. This includes creating new users, deleting users, and changing their permissions. Also referred to as keys to the kingdom, since account tends to have access to everything.
- **End of Life (EOL) -** An end-of-life product is a product at the end of the product lifecycle, indicating that the product is at the end of its useful life. At this stage, a vendor stops the marketing, selling, or provision of parts, services or software updates for the product.
- **Endpoint –** any device that is physically an end point on a network. Laptops, desktops, mobile phones, tablets, servers, and virtual environments can all be considered endpoints.
- **FileVault -** is a disk encryption program in Mac OS X 10.3 and later. It performs on-the-fly encryption with volumes on Mac computers.
- **Intrusion Prevention System (IPS) -** is a form of network security that works to detect and prevent identified threats.
- **Least Privilege** - is the idea that at any user, program, or process should have only the bare minimum privileges necessary to perform its function
- **Local Administrator** - In Windows, a local administrator account is a user account that can manage a local computer. Generally, a local administrator can do anything to the local computer but is not able to modify information in active directory for other computers and other users.
- **Passphrases** - A passphrase is a sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage but is generally longer for added security.

- **Personally Identifiable Information (PII) -** is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for deanonymizing previously anonymous data can be considered PII.
- **Privileged Account** - A privileged account is an account that has more privileges than ordinary users. Privileged accounts might, for example, be able to install or remove software, upgrade the operating system, or modify system or application configurations. They might also have access to files that are not normally accessible to standard users.
- **Privileged Access Management** - refers to a class of solutions that help secure, control, manage and monitor privileged access to critical assets
- **Security Information and Event Management (SIEM) -** is a subsection within the field of computer security, where software products and services combine security information management and security event management. They provide real-time analysis of security alerts generated by applications and network hardware.
- **Smishing -** is when someone tries to trick you into giving them your private information via a text or SMS message.
- **Software as a Service (SaaS) -** is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet.
- **Virtual Private Network (VPN)** – extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
- **Virtual Local Area Networks (VLANs)** – A virtual LAN is any broadcast domain that is partitioned and isolated in a computer network at the data link layer. LAN is the abbreviation for local area network and in this context virtual refers to a physical object recreated and altered by additional logic.
- **Vishing – "**voice phishing" is a form of criminal phone fraud, using social engineering over the telephone system to gain access to private personal and financial information.