CYBERSECURITY CHECKLIST FOR ORGANIZATIONS FROM AN INCIDENT RESPONSE PROFESSIONAL'S PERSPECTIVE

The following cybersecurity checklist has been prepared from a cybersecurity incident professional's perspective based on extensive experience in investigating cyber incidents. The checklist covers six common areas prone to intrusion and is meant to be a practical guide for organizations to raise cybersecurity awareness.

EideBailly®

CPAs & BUSINESS ADVISORS

1. EMAIL ACCOUNTS

FOCUS ON:	ASK THESE QUESTIONS:	YES	NO
MULTI-FACTOR AUTHENTICATION *Computer user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism.*	Does your organization require multi-factor authentication?	☐	☐
PASSWORD REQUIREMENTS *Passphrases are typically a sequence of words or other text to control access. Passphrases are typically longer and more sophisticated than passwords.*	Does your organization require a passphrase versus a traditional password?	☐	☐
	Does your organization require a frequent password change (e.g., 60 or 90 days)?	☐	☐
TAGGING EXTERNAL EMAILS *Tagging external emails is an important measure in helping identify spoofed domains. These tags create "red flags" for the email recipients and creates additional skepticism and cybersecurity awareness.*	Does your organization tag external emails and provide readily identifiable messages such as "Warning: This email originated from outside the organization"?	☐	☐
LOGS *Logs capture the who, what, when, where, why, and how about emails coming in and going out of the organization..*	Does your organization retain historical logs for one year or more?	☐	☐
	Does anyone in your organization actively review logs on a monthly basis for anomalous activity such as unusual Internet Protocol (IP) addresses or mailbox forwarding rules?	☐	☐

Go to Next Page

1. EMAIL ACCOUNTS (CONTINUED)

FOCUS ON:	ASK THESE QUESTIONS:	YES	NO
ADMINISTRATORS *Organizations typically assign global administrative rights to a user who can create, delete, and manage all inboxes within an organization.*	Are administrator accounts only used for administrative purposes?	☐	☐
	Are there adequate security controls in the organization to audit administrator account usage?	☐	☐
	Are there mechanisms in place to disable email accounts after employee turnover?	☐	☐
ANOMALOUS LOGINS *Many business email compromises (BEC) contain login activity not belonging to the intended user. Establishing normal activity identifies abnormal activity.*	Are both successful and failed logins examined for indicators of compromise or abnormal IP addresses?	☐	☐

Go to Next Page

2. COMPUTERS/SERVERS

FOCUS ON:	ASK THESE QUESTIONS:	YES	NO
PROACTIVE ENDPOINT MONITORING *Many critical data breaches are not detected by organizations until the threat actors make themselves known to the organization. Unfortunately, most of the activity a threat actor has performed on systems in order to have that level of control is detectable, but not detected due to inadequate monitoring mechanisms.*	Does the organization perform wide sweeps of endpoints on the enterprise with advanced technologies such as Next-Generation Antivirus (NGAV), Endpoint Detection Response (EDR), automated indicator of compromise signatures, and abnormal automated computer processes?	☐	☐
	Does the organization have the ability to perform incident response triage investigations on all computers on the enterprise easily?	☐	☐
	Does the organization have dedicated staff that is able to perform deep incident response tasks such as single host forensics and memory analysis?	☐	☐
MALWARE DETECTION *Phishing is the most common method to introduce malware into a system. Many times, phishing compromises an organization via social engineering techniques. However, there are many times phishing introduces malware with much more adverse effects.*	Does the organization have the ability to detect malware that may not have been detected by antivirus or automated scanning mechanisms?	☐	☐
APPLICATION/PATCH MANAGEMENT *Keeping systems and applications updated is a critical proactive cybersecurity step. Obtain, test and deploy software and firmware patches as quickly as practical and enable automatic updates whenever possible. Replace end of life (EOL)/unsupported operating systems, applications and hardware with vendor supported versions/models. Make it harder for attackers by eliminating known vulnerabilities.*	Does the organization inventory and manage hardware and software assets?	☐	☐
	Does the organization deploy standard baseline images to control hardware and software configurations?	☐	☐
	Does the organization have the ability to update/patch outdated and/or unsupported software using an application inventory solution?	☐	☐
	Does the organization have devices running end of life (EOL) operating systems?	☐	☐
VOLUME ENCRYPTION *Cybersecurity incidents are often confused with high-tech adverse hacker activity. A cyber incident can also be a lost or stolen computer device.*	Does the organization utilize full volume encryption technology to protect against stolen or lost computer devices?	☐	☐

Go to Next Page

2. COMPUTERS/SERVERS (CONTINUED)

FOCUS ON:	ASK THESE QUESTIONS:	YES	NO
MULTI-FACTOR AUTHENTICATION *Implementing best-practice access control for computer systems adds another layer of security to an organization's information.*	Does the organization facilitate the use of multi-factor authentication into computer devices?	☐	☐
ADMINISTRATORS *Organizations typically create administrator accounts on computer devices that are designed for technical support or environment management processes.*	Are administrator accounts only used for administrative purposes?	☐	☐
	Are local administrator accounts restricted from using software that has been known to be used for malicious purposes?	☐	☐

Go to Next Page

3. NETWORKS

FOCUS ON:	ASK THESE QUESTIONS:	YES	NO
AUTHORIZED ACCESS *Authorized access to certain sensitive information within your organization should be limited.*	Does your organization restrict access to certain folders, files, or applications?	☐	☐
	Does your organization monitor for unauthorized access to restricted folders, files, or applications?	☐	☐
LOGS *Logs capture the who, what, when, where, why, and how about incoming and outgoing network traffic.*	Does your organization retain historical logs for one year or more?	☐	☐
	Does anyone in your organization actively review logs on a monthly basis for anomalous activity such as unusual Internet Protocol (IP) addresses, system, file, or folder access?	☐	☐
NETWORK DATA TELEMETRY *Network data telemetry is sometimes the only evidence that shows evidence of data exfiltration. Without this telemetry, an organization may be unaware that threat actors may be stealing large amounts of data.*	Does the organization have the technology in place to gain visibility into network data flow as well as the ability to investigate this activity?	☐	☐
FIREWALL SECURITY *Firewall technology is an essential piece of network security. However, a firewall device without active security management and configurations can allow unwanted activity.*	Does the organization maintain firewall technologies and enhance the firewall security capability with incident threat intelligence?	☐	☐

Go to Next Page

4. MOBILE DEVICES

FOCUS ON:	ASK THESE QUESTIONS:	YES	NO
MOBILE DEVICE MANAGEMENT *Mobile user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence.*	Has your organization implemented a mobile device management (MDM) system to safeguard employee activity on the mobile devices that are connected to the organization's assets?	☐	☐
PASSWORD/PASSCODE REQUIREMENTS *Password/passcode typically consist of text, numeric, and/or special characters to prevent unauthorized access to a device.*	Does your organization require a password/passcode for all mobile devices, whether organization or employee owned, that are used for business purposes?	☐	☐
AUTHORITY *The purpose of a cybersecurity incident response investigation is to identify and document an incident vector (e.g., initial point of entry). Many times, an incident vector is created when a user clicks on a malicious link in an email from a personal mobile device.*	Does the organization have the appropriate authority to confiscate and examine personal mobile devices during an incident investigation?	☐	☐

5. DATA RETENTION/DESTRUCTION POLICY

FOCUS ON:	ASK THESE QUESTIONS:	YES	NO
DATA RETENTION/ DESTRUCTION POLICY *Organizations should have a data retention/destruction policy in place to mitigate the risk of data loss due to a cybersecurity incident.*	Does your organization have a formal data retention/ destruction policy in place covering data maintained within corporate emails accounts, computers, servers, networks, mobile devices, and applications?	☐	☐
	Does your organization enforce its data retention/ destruction policy?	☐	☐

Go to Next Page

6. ELECTRONIC FUNDS TRANSFER PROCESS/CHANGES

FOCUS ON:	ASK THESE QUESTIONS:	YES	NO
BANK ROUTING AND ACCOUNT CHANGES *Organizations will receive and/or send requests for changes inclusive of changes to bank routing and/or account information. Organizations should have a process in place to verify the requested change.*	Does your organization require physical verification (e.g. in person or via phone) of bank routing and/or account information before a change is executed?	☐	☐

CONCERNED YOU MAY HAVE ENCOUNTERED A POTENTIAL CYBERSECURITY INCIDENT?

WE CAN HELP! ➤➤➤