A Guide to Basic Controls Demonstrating Cyber Preparedness

MARCH 2022

The challenges created by the current cyber threat landscape continue to plague insurers, policyholders and prospective purchasers of cyber insurance. To qualify for cyber insurance, insurers require organizations to have certain basic controls and be prepared to respond and bounce back quickly in the event of a cyberattack.

This guide explains the major control categories that must be implemented to qualify for cyber insurance. These control categories are not an exhaustive list of all insurer requirements. Multiple factors are considered by each individual insurer when evaluating an organization. However, the consistent message from cyber insurers has been that the controls discussed in this guide are the ones they find most important at this time.

Access management

Polices and procedures employed by the organization to limit and restrict access to information, data, applications, processes, and platforms.

SAMPLE APPLICATION QUESTIONS

- How does the organization manage privileged accounts?
- How many users have persistent privileged accounts for servers and endpoints?
- How many service accounts does the organization have?
- How does the organization evaluate permissions for administrator accounts and service accounts?
- How often are privileges reviewed?

INSURERS' GENERAL BASELINE REQUIREMENT

Use tools (e.g., CyberArk, Thycotic Secrete Server, Iraje Privilege Access Manger, BeyondTrust Privileged Remote Access) that keep the accounts under "lock and key" — essentially a safe/vault to keep credentials for privileged accounts.

Limit the number of privileged accounts for critical systems and/or processes to one, but no more than two.

Establish a process to periodically review privileged accounts.

APPROACHES TO CONSIDER

- Employ principle of least privilege, i.e., provide users the least amount of permissions necessary to complete their job functions.
- Separate duties, i.e., critical functions should be divided amongst individuals and teams, such that no single individual has such broad access privileges that could lead to system compromise.
- Inventory all user accounts, types of accounts, and privileges regularly.
  - Domain Administrator Accounts are those that generally have rights to access and edit any solution, platform, application and/or processes in the organization's information technology environment.
  - Local Administrator Accounts are those accounts that have been established that allow the user to access and edit anything in relationship to the local device.
  - Service Accounts are those accounts specifically created to run automated solutions, applications, and processes, i.e., they facilitate a process and/or application without human involvement.

Multi-factor authentication

Means used to verify the identity of the user attempting to access any information, data, platforms and/or applications. Typically, these will involve a combination of something the user knows (e.g., password), something the user has (e.g., a token/verification code), and/or something the user is (e.g., fingerprint).

SAMPLE APPLICATION QUESTION

- Does the organisation have multi-factor authentication enabled on all user accounts?

INSURERS' GENERAL BASELINE REQUIREMENT

Enable multi-factor authentication for remote access, administrator accounts and email, and have at least two authentication measures in place, e.g., password and token.

Multi-factor authentication should be enabled for organisations using cloud based solutions to house sensitive information.

Examples: One-time passcodes (OTPs) sent to user by text message, email or phone call; software tokens; hardware tokens (commonly small thumb drives or keycards); mobile-push on a software application to a mobile device; biometric factors; and contextual or risk-based authentication, which look for certain criteria like location, device type and user patterns/behaviors.

Backup policies

Measures that duplicate the organization’s data and systems so that they can recreate the data and systems if there is an incident, instead of starting from the beginning.

SAMPLE APPLICATION QUESTION

- What are the organization’s standards for backups?

INSURERS’ GENERAL BASELINE REQUIREMENT

Backup critical information at least weekly, and segment and encrypt those backups.

APPROACHES TO CONSIDER

- Image backup which backs up the entire device, including settings and operating system, as well as files.
- File backup which only backs up files chosen.
  - NOTE: In order to restore this type of backup, a server/device must be built or already be capable of opening the files, so therefore it may take longer to restore from a file backup.
- Offsite storage with either cloud-based or physical server solution in another secure location without a persistent connection, i.e., the offsite storage should not be accessible from the organization’s network.
- The 3-2-1 rule :

3	2	1
One primary backup and two copies	Two different types of media to save the backups, e.g., a combination of server hard drive, external hard drive, cloud storage, and/or tape	One backup file maintained offsite

- Regular backup schedule. “Regular” is different for every organization but can be determined based on the recovery point objective (RPO), which is an organization’s chosen maximum length of time that data can be restored from, i.e., how much data can the organization lose/recreate in the event of an incident with minimal disruption? While constant, real-time backups are ideal, that may not always be an option, insurers may, at a minimum, require a weekly backup schedule.
- Encrypt backups — convert the backup such that it is not detectable and/or identifiable by those without authorization.
- Policies to ensure users only save on shared drives/file servers, i.e., users should not save critical business assets on their individual workstations, as well as accounting for data and information on personal devices used for business purposes, e.g., BYOD (Bring Your Own Device).

Blocking & filtering solutions

Mechanisms used to limit the potential for compromises as a result of malicious emails, links, websites, and other unauthorized attempts to gain access to the systems and network.

Perimeter blocking and filtering solutions

Tools that scan, filter and block malicious network activity, and can include an Intrusion Prevention System (IPS) deployed upon finding malicious activity and/or an Intrusion Detection Solution (IDS) which only detects and sends an alter to administrators in the event of suspicious activity.

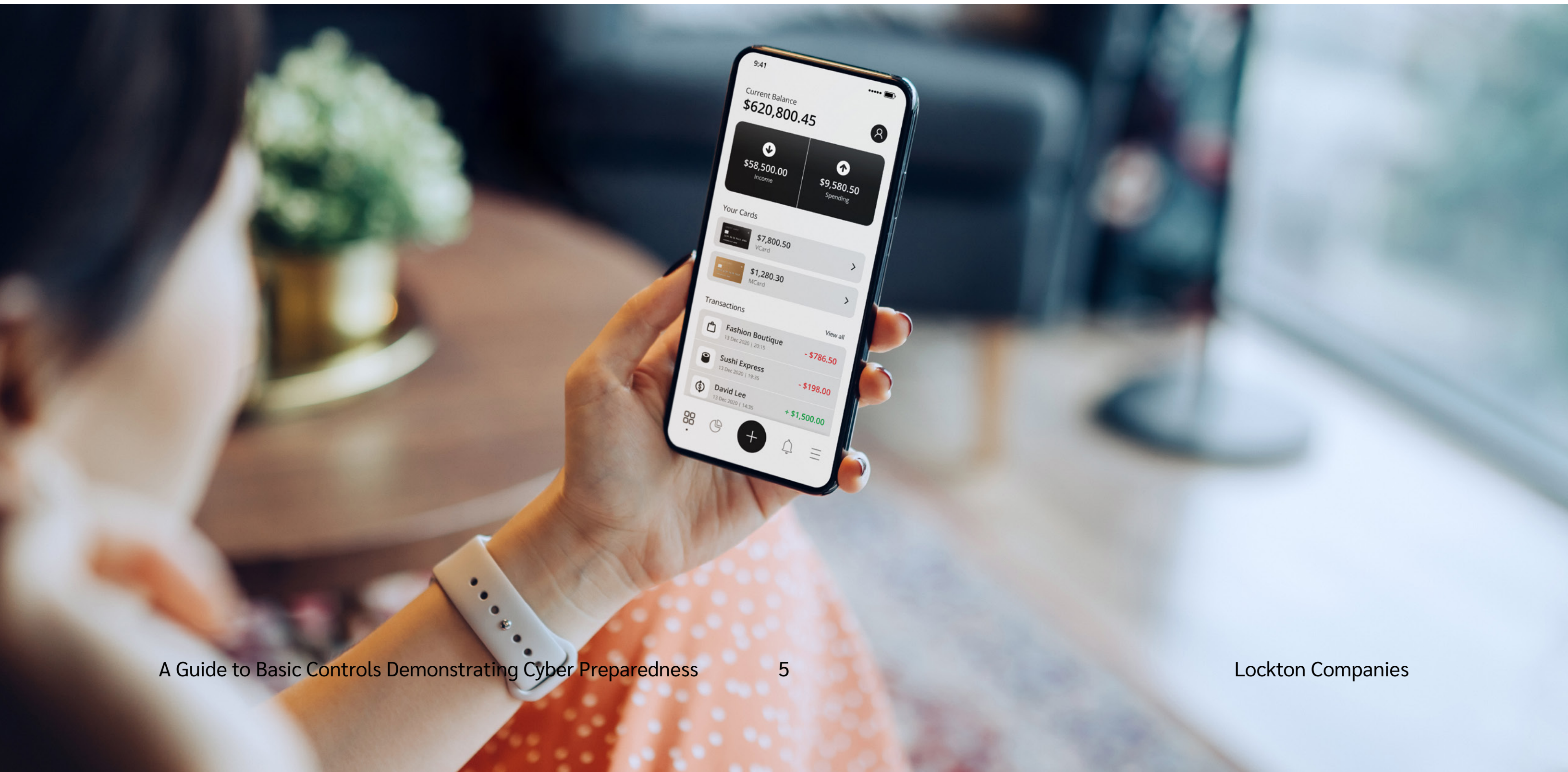
SAMPLE APPLICATION QUESTION

- Does the organization have an intrusion prevention or detection solution in place?

INSURERS' GENERAL BASELINE REQUIREMENT

Not mandatory at this time, but favorable consideration provided to those organizations using intrusion prevention or detection tools.

Examples: Cisco NGIPS; Corelight and Zeek; Fidelis Network; FireEye Intrusion Prevention System; Hillstone S-Series; McAfee Network Security Platform; OSSEC; Snort; ZScalar Cloud IPS; BlueVector Cortex; Vectra Cognito; Trend Micro Tipping Point



Email blocking and filtering solutions

Tools that block spam, phishing and viruses from reaching and/or leaving a user's email account and can include the following protocols:

- Sender policy framework (SPF) — allows organizations to define which IP addresses are allowed to send mail for a particular domain.
- DomainKeys Identified Mail (DKIM) — provides an encryption key and digital signature that verifies that an email message sent from the organization was not forged or altered.
- Domain-based Message Authentication, Reporting & Conformance (DMARC) — protects domains against abuse in phishing or spoofing attacks by validating the sender's identity within an organization's domain.

SAMPLE APPLICATION QUESTIONS

- Does the organization filter/scan incoming emails for malicious attachments and/or links?
- Does the organization have the ability to automatically quarantine, destroy and evaluate attachments?

INSURERS' GENERAL BASELINE REQUIREMENT

Use tools that block and filter emails to limit the potential for compromises as a result of a malicious email, link and/or attachment.

Examples: Mimecast; Secure Email Gateway; Topsec Email Security; Zerospam; SpamTitan; modusCloud; Hornetsecurity; and Sophos Email Security

Web blocking and filtering solutions

Systems that block access to malicious, dangerous or inappropriate content from websites.

SAMPLE APPLICATION QUESTION

- Does the organization route all outbound web traffic through a web proxy which monitors for and blocks potentially malicious content?

INSURERS' GENERAL BASELINE REQUIREMENT

Utilize a web proxy to limit the potential risks from everyday internet usage.

Examples: Websense; Bluecoat; and Forcepoint

Cybersecurity awareness & training

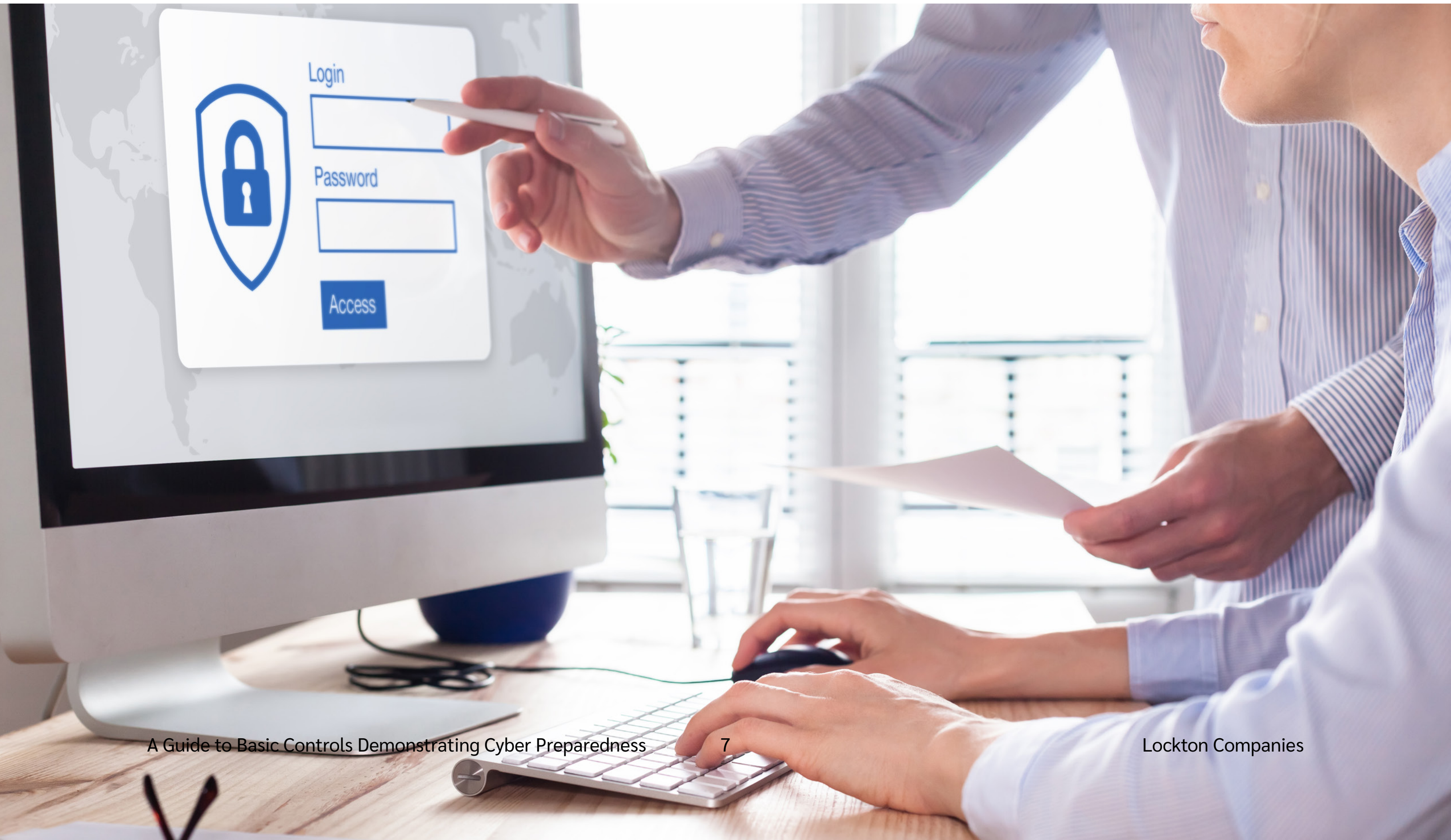
Policies and procedures to train an organization's workforce to ensure good cyber hygiene habits, increase awareness of risk and promote an organizational culture of mindfulness around cybersecurity and privacy rights. These policies can include simulated phishing attacks, training seminars and privacy compliance exercises.

SAMPLE APPLICATION QUESTION

- Does the organization simulate phishing attacks to test its workforce's cybersecurity awareness?
- Does the organization conduct mandatory information security and privacy training of employees and contractors?

INSURERS' GENERAL BASELINE REQUIREMENT

Test workforces' susceptibility to phishing attacks annually and implement annual training on cybersecurity and privacy protection compliance.



End-of-life support software

No longer receives patches/updates from the vendor and is extremely vulnerable to attacks. Without patching, threat actors have the ability to try to exploit vulnerabilities for a much longer period of time, often undetected.

SAMPLE APPLICATION QUESTIONS

- If organization has any end-of-life or end-of-support software, is it segregated from the rest of the network?
- Does the organization have a process to decommission unused systems?

INSURERS' GENERAL BASELINE REQUIREMENT

Identify, segment and establish a process for sunsetting and removal from inventory.

Endpoint detection & response tools (EDR)

Mechanisms used to secure end user devices, such as laptops and mobile phones. EDR tools are behavior focused, i.e., "should this application be doing this activity with this user at this time with these files"? EDR is not the same as antivirus software (e.g., Webroot, ESET, Bitdefender, McAfee) which looks for malicious files as compared to a known "clean" version of the same file.

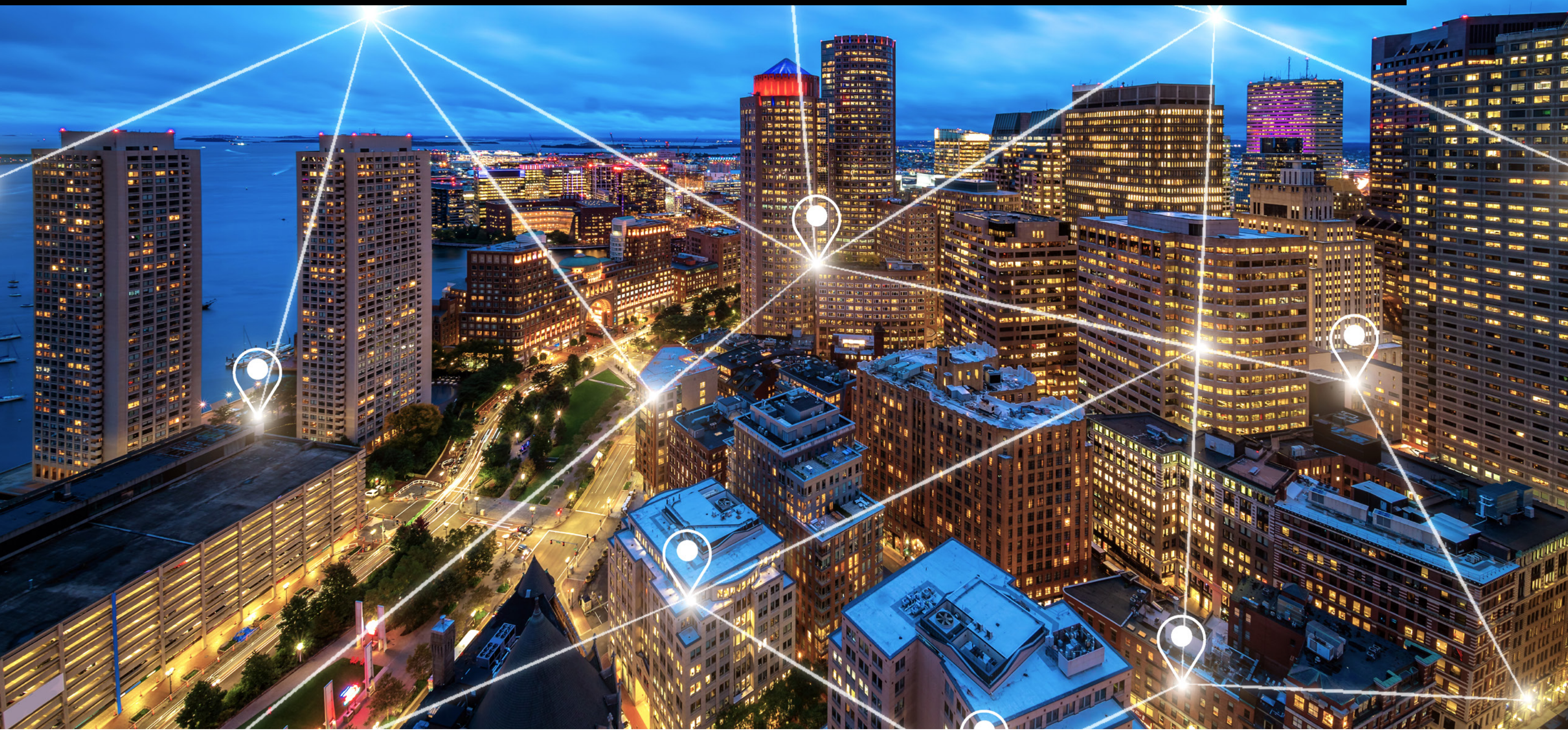
SAMPLE APPLICATION QUESTION

- Does the organization use an endpoint protection and response product across its workstations?

INSURERS' GENERAL BASELINE REQUIREMENT

Use detection tools to examine files as they enter the network and employ a product to respond to any malicious activity or threat source.

Examples: Symantec Endpoint Protection, Falcon by Crowdstrike, Singularity Platform by SentinelOne



Incident response and business continuity plans

Written policies that identify the key steps that will need to occur to: (a) respond to the incident; and (b) continue business operations in the event of an incident. These documents serve as the roadmap for responding to the incident and continuing business operations when an incident occurs. These plans should be printed and stored in multiple locations, so that they are accessible during an incident.

SAMPLE APPLICATION QUESTIONS

- Does the organization have a written incident response plan to address cyberattacks?
- Does the organization have a written business continuity plan to address cyberattacks?

INSURERS' GENERAL BASELINE REQUIREMENT

Written plans that are tested at least once a year to assess the ability to respond and restore critical systems, information, and operations.

Network and infrastructure segmentation

An architectural approach that divides a network into multiple segments or subnets, each acting as its own small network. While improving performance, more importantly, segmentation provides additional security, i.e., if a network is segmented a threat actor may be able to infiltrate one segment, the chances of infiltrating others and compromising the entire network are diminished.

SAMPLE APPLICATION QUESTIONS

- Does the organization segment its network based on certain criteria, such as: classification or level of information stored, geography and business function?
- Does the organization segregate critical networks from internet facing or other less critical networks?
- Does the organization segregate operational technology from information technology networks?

INSURERS' GENERAL BASELINE REQUIREMENT

Segment at multiple levels, including classes of information, business function and geography — specific requirements will vary by insurer, class of business and organization size.

Example: In a manufacturing plant, have human resources platforms, applications, information and data been segregated from operational technology (OT), the sensors and devices monitoring, tracking, and automating machine and systems functionality? In other words, if there is a compromise of the OT, will the manufacturing organization be able to communicate with customers and serve the needs of its workforce, including making payroll, ensuring accurate time keeping, and providing health and welfare benefits?

Patches/updates

Measures to protect software applications when a security flaw is discovered in them. The software developer typically creates a replacement program and/or file, i.e., "patch" to eliminate flaws discovered in earlier versions.

SAMPLE APPLICATION QUESTION

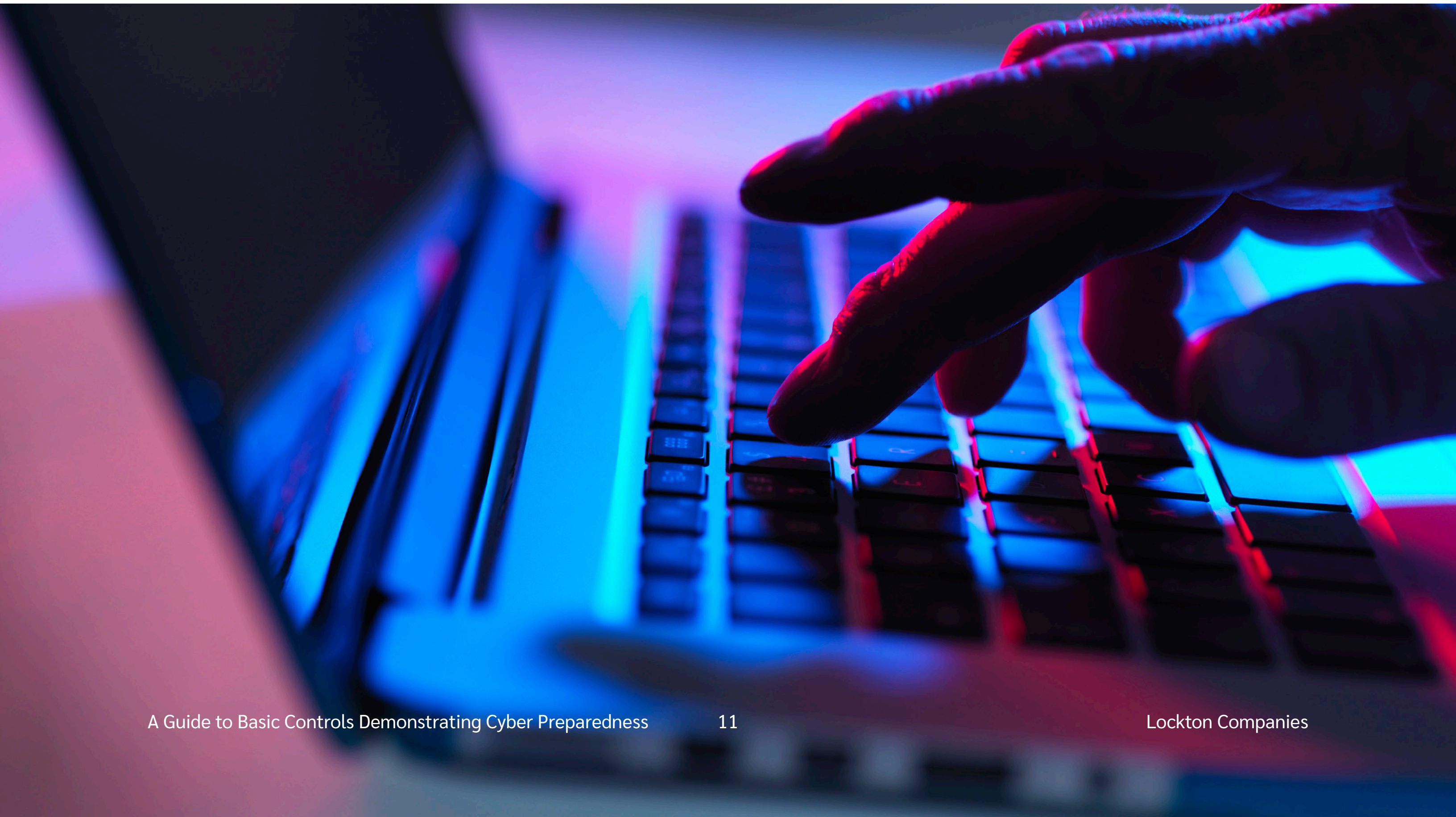
- What is the organization's timeframe to implement critical patches?

INSURERS' GENERAL BASELINE REQUIREMENT

Critical patches should be implemented within 24 to 72 hours with less critical patches being implemented within two to seven days.

APPROACHES TO CONSIDER

- Review all vendor communications regarding critical patches in a timely manner, i.e., within 24 hours.
- Establish a procedure regarding how patch notifications are received and deployed.
- Document any sandboxing, i.e., testing in a safe, isolated environment; additional assessments; and/or exceptions related to the patch/update.



Remote Desktop Protocol (RDP)

A Microsoft communication protocol that allows users access to their work desktops and administrators to diagnose problems remotely. It is among the most commonly exploited access points used by threat actors and should be blocked unless no other options exist, and additional protection is in place.

SAMPLE APPLICATION QUESTION

- If organization has enabled RDP, what tools are used to protect the network?

INSURERS' GENERAL BASELINE REQUIREMENT

Multifactor authentication is required if RDP is enabled.

APPROACHES TO CONSIDER

- Do not allow RDP connections over the open internet.
- Implement complex passwords.
- Employ multifactor authentication.
- Use an RDP Gateway, which provides a secure, encrypted connection via RDP, rather than an open, direct connection.
- Establish a procedure to lock out users and block or timeout Internet Protocol (IP) addresses that have too many failed logon attempts.
- Utilize a firewall to restrict access.

Security monitoring

Mechanisms employed by the organization to actively monitor security and can include a Security Incident Event Management (SIEM) system which collects and analyzes aggregated log data from the organizations network and platforms and a Security Operations Center (SOC) which consists of people, processes, and technology designed to address logged security events.

SAMPLE APPLICATION QUESTIONS

- Does the organization utilize a SIEM monitored 24/7 by a SOC?
- Does the organization have staff dedicated to monitoring security operations?
- Is that staff available 24/7?
- Does the organization outsource its security operations to a third party?
- Does the organization monitor active directory or have an identity and access management platform to detect unusual activity or abnormal behavior?

INSURERS' GENERAL BASELINE REQUIREMENT

Use SIEM and/or SOC to proactively monitor, identify, contain and mitigate any abnormal activity.

This guide is for educational and informational purposes only. Please consult your Lockton Cyber & Technology account executive to assist you with the specifics of your cyber insurance purchasing needs. If you do not have a designated Lockton Cyber & Technology account executive, please contact cyber@lockton.com for further assistance.

LOCKTON®

lockton.com |