Recommended Cyber Security Standards

In recent years, cyber-attacks have become increasingly sophisticated with threat actors constantly finding new ways to exploit vulnerabilities and avoid detection. As cyber-attacks continue to increase in complexity, the arms race between cyber criminals and security controls wages on with insurers looking for insureds to have controls in place that they deem “mandatory”, to mitigate the known and commonly exploited weaknesses.

Below we have outlined a list of risk controls which are either minimum standards for the cyber insurance market or highly recommended.

MFA and Access Management

Ensure both employee and all other 3rd party access to the network is secured using push-based multi factor authentication (MFA) (a code generated on a separate device). Further, access by any third-party ought to be closely monitored, also ensuring the ability to record and close the connection at any time. If RDP is used, connections should be via a VPN only, in addition to the MFA requirements. RDP should not be externally facing. Push-based MFA should also be in place for all administrator accounts, access to any critical information and remote access to emails.

Privilege Access Management

A dedicated Privilege Access Management (PAM) tool should be in place to manage all usage of administrator and privilege accounts. Access to PAM should use MFA and ideally be linked to a change control system. Local administrative accounts should be disabled, and domain administrator accounts should not have access to the internet or any email. All admin users’ activity should be monitored and logged. Service Accounts should be reduced to a minimum and ideally managed by the PAM tool.

In the absence of a dedicated PAM tool, permanent administrator accounts should be kept to a minimum, utilising complex and separate (and frequently rotated) login credentials.

Network Segregation

Network segregation between critical and non-critical information should be in place with further segregation between business units or geographical locations to prevent any lateral network movement. Any operational technology should be kept entirely separate from the IT network, with internet and external access blocked. Any legacy or end-of-life (EoL) software and hardware should be kept segregated from the wider network with no internet or external access, with a plan in place to decommission any EoL assets.

EDR and Network Monitoring

The use of Endpoint Detection and Response (EDR) or Managed Detection and Response (MDR) across 100% of endpoints including laptops, desktops and servers is required, with an endpoint protection platform (EPP) highly recommended. Any information from these services should be fed into a Security Information and Event Management (SIEM) system which is monitored 24x7 by a Security Operations Centre (SOC) either internally or externally. Regular network penetration testing and vulnerability scanning is also required with any issues remediated in a timely fashion.

Data Backups

Regular backups should be immutable, encrypted and subject to vulnerability scanning and should be tested regularly for their integrity. Backups should also be physically and logically separated from the network and, if using a cloud or online service, subject to MFA with access limited only to specific administrator accounts.

Planned Responses

Incident response, business continuity and disaster recovery plans for recovery from cyber events with specific responses to ransomware attacks and data breaches should be in place, updated, and rehearsed regularly.

Employee Awareness and Education

Ensure employee security awareness training (including regular phishing simulations) are in place and deployed regularly. Protocols should be in place regarding the safe use of portable devices, limited use of public Wi-Fi, and security controls around video-conferencing.

Patching

Ensure all patches are implemented in a timely manner. Critical patches as defined by the CVSS scoring should be implemented as soon as possible, ideally within 72 hours of the patch release, highs within 7 days and medium/lows as business permits.

Carlo Ramadoro
Senior Vice President, Global Cyber & Technology
T: +44 020 7933 2431
E: carlo.ramadoro@lockton.com

Alex Spensley
Account Executive, Global Cyber & Technology
T: +44 020 7933 1354
E: alex.spensley@lockton.com

LOCKTON®

UNCOMMONLY INDEPENDENT