Alliant

Public Entity, Education & Pooling

System Security Standards Guidelines for Cyber Quotes

January 2023

As the cyber insurance market continues to change, we have updated this summary of commonly requested system security standards needed to obtain a quote. Please note that each carrier has its own nuances and this document is not a "one size fits all" as organizations will have different exposures and will fall into or out of the appetite of different underwriters but this is generally what we are seeing in the marketplace. Of course, more scrutiny will fall on larger organizations.

MFA 100% implemented for remote access and privileged user accounts.

Minimum: MFA implemented for access to email (e.g. enforced via Office 365. Note, if using O365, enabling Advanced Threat Protection is also a recommended standard).

Minimum: MFA enforced for access to "privileged user accounts" (i.e., the information technology department).

End-point protection, detection, and response product implemented across enterprise.

Minimum: an End-Point Protection (EPP) solution in place.

- Preferred: an End-Point Detection & Response (EDR) solution in place (Now considered a minimum on medium-large sized organizations)

If Remote Desktop Protocol connection enabled, the following are implemented:

Minimum: MFA-enabled VPN is used for access to any Remote Access software.

- Network level authentication enabled

Backups

Minimum: regular backups are (i) in place, (ii) successful recovery is tested, (iii) backups are stored separately (i.e. 'segregated') from the primary network, (iv) encrypted, and (v) protected with anti-virus or monitored on a continuous basis.

- Tested at least twice per year
- Ability to bring up within 24-72 hours – less time for critical operations (4-8 hours)

Planning & Policies

Minimum: Tested (rehearsed) Incident Response, Disaster Recovery & Business Continuity plans are in place.

- Incident Response Plan
- Disaster Recovery Plan
- Business Continuity Plan

Training

Minimum: training and regular simulated phishing exercises for all users.

- Social Engineering Training
- Phishing Training
- General Cyber security training
- Training of account team staff on fraudulent transactions

Patching

Minimum: Critical & high severity patches installed within 30 or fewer days, optimally within 1-7 days for critical & high severity patches regarding active exploits.

Miscellaneous

- Plan or have adequate measures in place to protect end of life software
- Sufficient IT Security budgets and dedicated security personnel, carriers generally like to see 10% of total IT spend go to security but this will differ based on organization size.
- Email Security controls in place
- Privileged Access Management. A PAM solution is now considered a minimum on medium-large sized insureds
- Service Account Management. What controls are in place to protect against loss from a compromised service account?

Please note this list is context-dependent.

If an underwriter views a client as potentially higher risk (e.g. due to previous incidents/losses) then they may look for more beyond the 'minimums'.

If the market continues to harden, underwriters 'minimum' expectations may increase in the future.

Different insurance carriers may have different expectations of 'minimums'. This is our current best understanding.

Many carriers are no longer writing new Public Entity business, regardless of controls.

Protecting your organization against ransomware

Minimum protection

- **Deploy and maintain a well configured and centrally managed End-Point Protection (EPP) solution:** A robust EPP/anti-virus solution is a basic component of any security program.
- **Email tagging:** Tag emails from external senders to alert employees of emails originating from outside the organization.
- **Email content and delivery:** Enforce strict Sender Policy Framework (SPF) checks for all inbound email messages, verifying the validity of sending organizations. Filter all inbound messages for malicious content including executables, macro-enabled documents and links to malicious sites.
- **Office 365 add-ons and configuration:** Enable two-factor authentication (2FA) on Office 365 and use Office 365 Advanced Threat Protection.
- **Macros:** Disable macros from automatically running. Ideally disable them from running at all if your business does not need them.
- **Patching:** Conduct regular vulnerability scans and rapidly patch critical vulnerabilities across endpoints and servers – especially externally facing systems.
- **Remote Access:** Do not expose Remote Desktop Protocol (RDP) directly to the Internet. Use Remote Desktop Gateway (RDG) or secure RDP behind a multi-factor authentication-enabled VPN.
- **Media usage controls:** Put in place controls on the insertion and/or use of media which does not carry appropriate authentication/media identifiers.
- **Well-defined and rehearsed incident response process:** Helps mitigate losses and rapidly restore business operations after a ransomware attack.
- **Back-up key systems and databases:** Ensure regular back-ups which are verified and stored safely offline.
- **Educate your users:** Most attacks rely on users making mistakes, train your users to identify phishing emails with malicious links or attachments. Regular phishing exercises are a great way to do this.
- **Firewalls**: Use network and host-based firewalls with well considered rule-sets, for example, disallow inbound connections by default.

Stronger protection

- **Establish a secure baseline configuration:** Malware relies on finding gaps to exploit. A baseline configuration for serves, end-points and network devices that conforms to technical standards such as Center for Internet Security (CIS) benchmarks can help plug those gaps.
- **Filter web browsing traffic:** Web filtering solutions will help prevent users from accessing malicious websites.
- **Use of protective DNS:** Helps deny access to known malicious domains on the Internet.
- **Manage access effectively:** Ransomware doesn't have to go viral in your organization. Put in place appropriate measures for general user and system access across the organization: privileged access for critical assets (servers, end-points, applications, databases, etc.) and enforce multi-factor authentication (MFA) where appropriate (remote access/VPN, externally facing applications, etc.)
- **Regular testing of back-ups:** Reduces downtime and data loss in the case of restoring from back-ups after a ransomware attack.
- **Disconnect back-ups from organization's network:** Prevents back-ups from being accessed and encrypted by ransomware in case of a successful attack on an organization's main network.
- **Separately stored, unique back-up credentials:** Prevents bad actors from accessing and encrypting back-up data.

Best protection

- **End-point detection and response (EDR) tools:** EDR solutions monitor servers, laptops, desktops and managed mobile devices for signs of malicious or unusual user behavior/activity. These tools also enable near immediate response by trained security experts. When effectively deployed and monitored, EDR tools are one of the best defenses against ransomware and other malware attacks.
- **Intelligent email evaluation:** Automatically detonate and evaluate inbound attachments in a sandbox environment to determine if malicious prior to user delivery.
- **Centralized log monitoring:** Centralized collection and monitoring of logs, ideally using a Security Information and Event Management (SIEM) system, identifies threats which breach your internal defenses.
- **Subscription to external threat intelligence services:** Provides access to external services that can provide details of developing attacker tactics, techniques and procedures. They also provide access to databases of known bad websites, mail attachments, etc.
- **Encrypted back-ups:** Prevents use of back-up data by bad actors.
- **Network segregation:** control access and/or traffic flow within the network environment. A well-configured firewall rule set will ensure that only the required traffic can flow from one segment to another. Furthermore, segregate end of life/support systems/software as a priority.
- **Web isolation:** Use of a web-isolation and containment technology to create a secure Internet browsing experience for your users.
- **Application permissions:** Only permit applications trusted by your organization to run on devices.

Lodestone SECURITY

Lodestone Security can help you make impactful changes to your security posture to either prevent breaches before they occur or prevent recurrences. For additional information:

James Habben – Director, Business Development
info@lodestonesecurity.com

KPMG

KPMG offers a wide range of services to help organizations defend against and respond to ransomware attacks.
To discuss how they can help please contact:

Matthew Martindale – Partner, Cyber Security
cyber@kpmg.co.uk

beazley