The Cyber Security Best Practices to Obtain Cyber Insurance for Larger and Higher Risk Organizations

Insurance carriers increasingly look for and even require companies to implement specific cybersecurity practices to qualify for coverage.

These requirements are not universal across all carriers; sometimes, a company can secure coverage without all these requirements. But aligning to these best practices will ensure a company gets the most and best-priced market coverage options.

Please Note: These best practices are applicable for larger organizations ($20mn+ revenue) or deemed higher risk for cyber attacks or those with prior cyber incidents. Smaller or lower-risk organizations should refer to our "Basic Cyber Security Requirements Needed to Obtain Cyber Insurance" guide for the basic requirements.

The Expanded Cyber Security Best Practices Checklist:

EMAIL SECURITY

- [ ] Turn on Multifactor Authentication for all users of the email system
- [ ] Tag external emails to alert employees that a message originates from outside the organization
- [ ] Deploy an email protection solution to prescreen emails.
- [ ] Deploy a specific email security provider
  - Recommended solutions include: Avanan, Barracuda, Cisco, Microsoft Defender, Mimecast, Proofpoint, SonicWall, Symantec, Trend Micro, or similar solution
- [ ] Deploy an email security solution to automatically detonate and evaluate all attachments in a sandbox to determine if they are malicious before delivery
- [ ] Implement the following to protect against phishing messages: Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain Based Message Authentication Reporting and Confirmation (DMARC)
- [ ] Remove access or enforce MFA for all email access on the web application or non-corporate devices
- [ ] If you use Microsoft Office 365, Enable the Advanced threat protection to add on

CLOUD AND DATA PROTECTION

- [ ] If you use a cloud provider to store data and host applications, ensure they are large, reputable, and have proper controls. (AWS, Azure, Google)
- [ ] Use MFA to secure all cloud provider services
- [ ] Encrypt all sensitive and confidential data on your systems and networks
- [ ] Where that is not possible, segment servers with sensitive and confidential data and put in place access control with role-based assignments
- [ ] Remove all remote access to your networks or use MFA to secure all remote access, including any RDP

AUTHENTICATION AND MFA

- [ ] Deploy Multi-factor Authentication (MFA) for all admin access and privileged accounts
- [ ] Deploy MFA on any remote access, including any RDP connections
- [ ] Use a reputable and trusted MFA provider
  - Recommended Solutions include: Auth0, Duo, LastPass,Okta, & OneLogin
- [ ] Use an MFA type that is ideally not SMS or push-based
- [ ] Ensure that your MFA configuration is set up such that the compromise of a single device will only compromise a single authenticator
- [ ] Deploy a privileged account management software
  - Recommended solutions include: CyberArk & BeyondTrust
- [ ] Monitor all administrator access for unusual behavior patterns

ASSET TRACKING AND CONFIGURATIONS

- [ ] Deploy hardened baseline configurations across all servers, laptops, desktops, and managed mobile devices
- [ ] Record and track all software and hardware assets deployed across the networks

BACKUPS

- [ ] Deploy offsite or cloud backups for all critical data and systems
- [ ] Assure those critical systems, applications and processes can recover in 10 days or less
- [ ] Use backups that continuously test restore to a virtual machine to assure the integrity and viability of the backups
- [ ] Encrypt your backups
- [ ] Use "immutable backups" that cannot be changes

NETWORK SECURITY

- [ ] Use protective DNS to block access to known malicious websites
  - Recommended tools include ZScaler, Quad6, and OpenDNS)

MONITORING AND RESPONSE

- [ ] Utilize a SIEM of SOC Solution
- [ ] Have an outsourced SOC Monitored 24-7

PATCHING

- [ ] Implement a vulnerability management tool
  - Recommended solutions include: Insight/VM/Rapid7, Nessus/ Tenable, & Qualys
- [ ] Have a formal 30-day patching cadence, with critical and zero-day patching applied within seven days.
- [ ] Remove all end-of-life or end-of-support software
  - If not possible, segment these from the rest of the network

APPLICATION SECURITY

- [ ] Remove all local admin rights from all non-IT users
- [ ] Remove the ability to run Microsoft Office Macro-enabled documents on their system by default
- [ ] Use endpoint application isolation and containment technology on all endpoints

Recommended tools include:

- [ ] Implement PowerShell best practices as outlined in the Environmental Recommendations by Microsoft

ENCRYPTION

- [ ] If the applicant is a retailer, restaurant, or online retailer, deploy end-to-end or point-to-point encryption on all point-of-sale (POS) terminals

Recommended but not required:

- [ ] Encrypt all sensitive information at rest
- [ ] Encrypt all sensitive information on mobile devices & laptops

ENDPOINT SECURITY

- [ ] Deploy an endpoint detection and response (EDR) solution

Recommended solutions include:

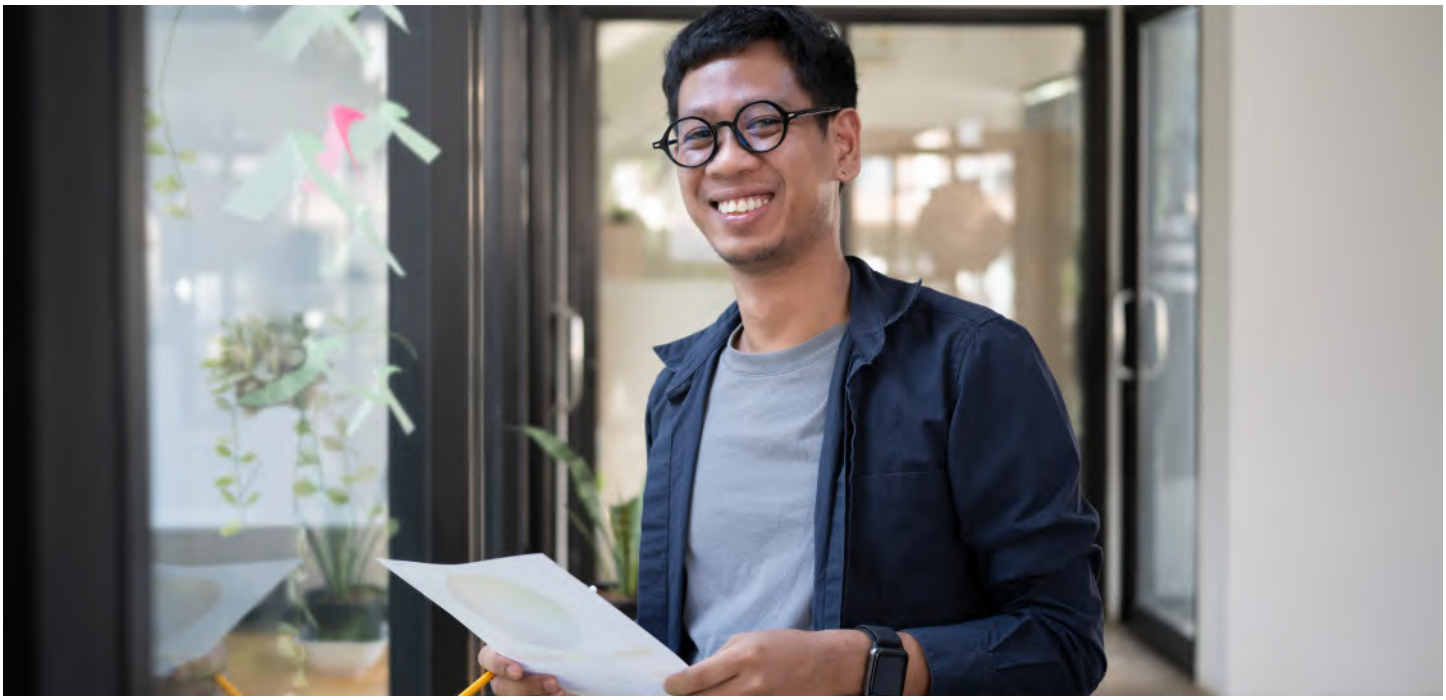
- [ ] Use an EDR solution that provides for centralized monitoring and logging of all endpoint activity across your enterprise
- [ ] Enforce application whitelisting/ blacklisting
- [ ] Deploy EDR across 100% of endpoints, including mobile devices and BYOD, if they can access the corporate network

SECURITY AWARENESS TRAINING

- [ ] At least annually, do security awareness training for all employees that include social engineering and phishing simulation
- [ ] At least annual training for executives and key accounting on fraudulent transfer schemes

PROCESSES AND PROCEDURES FOR WIRES AND FUNDS TRANSFERS

- [ ] Put in place controls that require all funds and wire transfers over $25k to be authorized and verified by at least two employees before execution
- [ ] Prevent unauthorized employees from initiating wire transfers
- [ ] Verify vendor/supplier bank accounts before adding them to accounts payable systems
- [ ] Require out-of-band authentication before the execution of all electronic payments



For more info:
partners@datastreaminsurance.com | www.datastreaminsurance.com