The Basic Cyber Security Requirements Needed to Obtain Cyber Insurance

Insurance carriers increasingly require companies to implement basic cyber security practices to qualify for coverage.

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

Please Note: These basic requirements are applicable to smaller and lower risk organizations. Organizations that are larger ($20mn+ revenue) or deemed higher risk for cyber attacks should refer to our "Cyber Security Requirements Needed to Obtain Cyber Insurance For Larger/Higher Riskier Organizations" guide.

The Basic Requirements Checklist:

EMAIL SECURITY

- [ ] Turn on Multifactor Authentication for all users of the email system

Recommended but not required:

- [ ] Deploy an email protection solution to prescreen emails.

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

Recommended but not required:

- [ ] Use backups that continuously test restore to a virtual machine
- [ ] Use "immutable backups" that cannot be changes

NETWORK SECURITY

- [ ] Deploy Multi-factor Authentication (MFA) for all admin access and on any remote access

PATCHING

Recommended but not required:

- [ ] Have a formal 30-day patching cadence, with critical and zero-day patching applied within seven days.

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

Recommended but not required:

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

SECURITY AWARENESS TRAINING

Recommended but not required:

- [ ] At least annually, do security awareness training for all employees
- [ ] 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

Recommended but not required:

- [ ] 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