POLSINELLI | What a law firm should be.™

Cybersecurity Insurance: Practical Steps Your Business Can Take to Become More Insurable

With the global average cost of a data breach now $4.45 million, a 15% increase over the past three years,[i] it is not a surprise that businesses have shown an increased interest in cybersecurity insurance amid frequent news of computer hacking, network intrusions, data theft and high-profile ransomware attacks.

At the same time, there is a range of insurance policies that may cover aspects of cybersecurity incidents and crime, like stand-alone cyber policies, E&O policies, commercial general liability, D&O/management liability, commercial crime coverage, media liability, network security and privacy policies, and other blended products.

However, insurers have started writing exclusions for cyber and privacy liabilities into "non-cyber" policies and directing policyholders to buy cyber insurance specifically for those risks. **Thus, it is more important than ever for businesses to have a clear understanding of whether their current policies cover cyber incidents and, if so, to what extent. And if not, what can your organization do as a company to make it more attractive to insurers?**

Practical Internal Steps

1. ***Security Awareness Training*.** We have all heard that employees are your company's greatest risk point. But with regular, documented training sessions, you can reduce this risk by educating and empowering your employees to prevent and detect common cyber threats. This also promotes a "security-aware mindset" that can have ancillary benefits. Many insurers partner with cyber-training firms and may offer them to your company at no cost. The key to success with these trainings is to be frequent and consistent.

2. ***Conduct Full Data Backups*.** You won't have to pay money to a cybercriminal if you have another copy of the data they are holding for ransom. The goal of regular data backups is to allow businesses to continue operating even if data is compromised. Regularly backing up all of your business data, whether it is on-premises or in the cloud, is the ultimate safety net.

3. ***Automate Passwords/Use MFA*.** Because most cybercriminals depend on stolen user credentials to access a private network, automated passwords and use of multifactor authentication ("MFA") could disrupt a majority of network compromise attempts. Microsoft has even gone so far as to say it would prevent 99.9% of them![ii] MFA is the process of using at least two pieces of evidence to confirm a user is who she is supposed to be (usually a password plus a one-time password or code sent to the user's phone or email). Additionally, employ a password manager to help keep track of multiple passwords and generate new passwords at random. This cuts down on employees using the same passwords for multiple platforms or writing those passwords down.

4. ***Establish a Vendor Management Process*.** The greatest data privacy threat companies actually faced in 2023 was their upstream and downstream vendors, with 63% of all data breaches being tied to or directly caused by vendors. Many companies rely on their procurement department to gather information and negotiate with vendors. This may be fine outside of the cyber context, but when it comes to IT, software and other vendors that have cloud-based or "connected" solutions, additional vetting and contracting processes must be employed to properly assess and mitigate the risks your vendors pose to you.

Practical External Steps

5. ***Conduct Penetration Testing & System Audits*.** It is important to test your company's systems, network and technical infrastructure so you find the vulnerabilities before a cybercriminal does. Often, companies that can show regular system scans and audits done by a reputable third party enjoy a break in their cyber premiums. Penetration testing is an authorized, simulated attack on your IT systems. It should be designed to mimic the techniques a cybercriminal would use to determine the efficacy of your company's security controls.

6. ***Consult a Managed Service Provider*.** Utilizing a third-party security professional, or managed service provider ("MSP"), to help your company better plan, monitor and secure its digital environment is an excellent way to bolster your protections. MSPs can offer 24/7 system monitoring and proactive threat detection as well as compliance management. An MSP may identify a blind spot your company did not have on its radar. And as there is a crowded market for these services, they can often be the same price or less expensive than having a captive team of employees doing all of these tasks.

7. ***Draft an Incident Response Plan*.** No Incident Response Plan ("IRP") can guarantee the prevention of a data breach, but a well-drafted and well-rehearsed IRP can significantly minimize the impact a cyber incident has on your company. IRPs outline company procedures to follow and individual roles to engage in the event of an incident. Organizations with comprehensive IRPs had approximately $2.66 million less in damages and costs than those that did not have an IRP in place.[iii] Companies that have an IRP should review it annually. Tabletop cyber exercises bring all of the key players into the same room and have them act out what their roles and responsibilities would be if an incident were to take place. Some insurers will offer their clients a facilitator who can guide

the company through this exercise. Other professional organizations should be present as well, including any MSP you have engaged and your trusted law firm partner.

With cyber insurance premiums going up and policy limits going down, as well as a consolidation of cyber insurance providers in the market, insurers want to see that their clients are engaging in industry-standard preventive measures.
Taking advantage of these practical steps will not only make companies more attractive to insurers but also improve the security posture of the company in the process, which lowers the company's need to ever claim on that policy in the first place.

---

[i] https://www.ibm.com/reports/data-breach

[ii] **https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/**

[iii] https://www.ibm.com/reports/data-breach