Not if, But When

Mitigating Data and Cybersecurity Risk

Sandra Moody Gresham,

In today's data-driven world, businesses and organizations of all sizes are at risk of data breach or a cybersecurity attack. It is no longer a question of if your organization will suffer a breach, but more so, when. Just one stolen laptop, one resourceful hacker or rouge employee, or one virus can create enormous financial and reputational consequences. And, your commercial general liability or umbrella policy is not likely to cover the wide ranging costs associated with such a breach. With an average cost of a compromised record now totaling $217 per the Ponemon Institute, these risks continue to grow in expense and sophistication. Though we're familiar with the publicized data breaches of companies like Anthem, Target, Google, JP Morgan Chase and the federal Office of Personnel Management, more than a third of all cyber security breaches affect firms with fewer than 100 employees.

"businesses should stop worrying about preventing intruders getting into their computer networks, and concentrate instead on minimizing the damage they cause when they do."

So what is data breach and cybersecurity? Data breach occurs when Personal Identifiable Information (PII) is exposed, stolen or comprised due to unauthorized use. PII could include birthdates, social security numbers, credit card numbers, bank account numbers or medical records, etc., of customers or employees. This data can be breached in a myriad of ways with some of the most common breaches involving hacking, lost or stolen laptops/devices, employee errors, ransomware, and hacktivism. Cybersecurity risk or cyber attacks are criminal activities conducted via the Internet. These attacks can include stealing an organization's intellectual property, confiscating online bank accounts, creating and distributing viruses on other computers, posting confidential business information on the Internet to disrupting a country's critical national infrastructure. Cyber attack losses are costing companies worldwide an average of more than $7.7 million annually in legal defense costs, legal settlements, lost business revenue, customer notification costs and more.

Cyber liability insurance is designed to provide protection to cover direct and indirect costs associated with a breach or cyber attack.

Though policies are different and there is no current standardization, today's policies provide many of the below coverages:

- **Notification and Credit Monitoring Expenses**, to assistance in compliance with statutory mandates to notify individuals of a loss or theft of PII and credit monitoring services.
- **Data Privacy Liability**, protects against claims alleging that the insured's negligence resulted in the breach or violation of law due to the unauthorized access or unauthorized use of computer systems.
- **Network Security Liability,** provides protection against claims alleging that your negligence resulted in failure to prevent unauthorized access or unauthorized use of a third-party's computer system.
- **Cyber Investigation Expense**, covers services provided by a third-party vendor to investigate and determine the source or cause of a data privacy wrongful act or network security wrongful act.
- **Crisis Management, Business Interruption and Data Restoration**, provides assistance to help restore comprised systems and cover public relations expenses.

James Lewis, a cybersecurity expert from Washington's Center for Strategic and International Studies (CSIS), states, "businesses should stop worrying about preventing intruders getting into their computer networks, and concentrate instead on minimizing the damage they cause when they do." The potential for cyber event is real regardless of the size of your organization and the worst thing your organization can do is ignore the risk.

DEHAN ENTERPRISES INSURANCE & FINANCIAL SERVICES LLC
762 E Main Street Columbus Ohio 43205 614 238-3520 (o) 614 586-1719 (fax) info@dehaninsurance.com