Aon CyberBusinessPro℠
DATA EXPOSURE RESPONSE PROTECTION

# Cyber Risk FAQs

## The Basics

### *What is data and cyber risk?*

Every business has data that can be damaged, lost or stolen. Computer systems and networks can also be attacked and damaged/destroyed. Data and cyber risks arise from the use of computer systems and the collection, use and storage of data, both electronically and on paper. Accidents and malicious attacks involving systems and data can be devastating to a business. And, with proprietary and/or personal data being such a valuable asset, criminal attacks have become commonplace in businesses of all sizes, large and small.

### *What are some examples of the risks faced by small businesses?*

Risks and exposures exist wherever information is collected. Sensitive, personally identifiable information (PII) of customers on computer systems, laptops, smart phones, external (thumb) drives, cloud data providers and paper office files all contain data that is very valuable to ID thieves and hackers. It's also susceptible to loss through negligence or accidents. Similarly, data in transit via email, web browsers and even the postal service is exposed. Data held by vendors, independent contractors or work-from-home employees are also exposures. Data breach incidents can occur as a result of negligence of trusted employees, the lack of data security, and malicious hacking from ID thieves or rogue employees.

Regardless of how data is lost or destroyed, the current landscape presents risks to every organization that loses data that is within its care, custody and control.

### *How can an organization address the risks?*

Information security best practices and cyber risk management is essential to identify and minimize risks. Employee / management education, heightened security policies, procedures, and technology defenses are all important, as well as network security. However, no organization can ever be 100% secure from fraud, which makes Cyber Liability insurance a vital layer of security when other security measures have failed.

### *What is Cyber Liability Insurance?*

Cyber Liability insurance provides financial protection for data and electronic cyber risks. Computer systems can be damaged and destroyed, and data can be lost, stolen and compromised. However, unlike other physical exposures, data is not tangible. This intangible exposure, which is not covered by traditional insurance coverage, gave rise to the first "cyber" or data risk insurance policies that date back to the mid 1990's.

### *Isn't this covered by a General Liability policy?*

No, not unless specifically endorsed. Traditional general liability policies (ISO policy forms) are now specifically excluding cyber risks.

### *How does cyber risk affect my small business?*

Like any physical risk not covered by insurance, having an uncovered data related loss can be catastrophic. A National Cyber Security Alliance study found that 60 percent of small firms go out of business within six months of incurring a data breach.[1] Although most small organizations do a good job of managing their traditional physical risks (fire, theft, windstorm, general liability, etc.) they don't generally understand the exposure relating to intangible risks of data theft and cyber liability. These are all very real exposures affecting small and medium-sized businesses all over the country, and they need to be addressed.

### *Why should a small business buy this coverage?*

Many individuals and businesses have a mindset that "it won't happen to me". However, industry statistics indicate small businesses are being attacked at alarming rates, in part, due to the relative ease of theft and abuse. A report by *Symantec* found that small businesses accounted for more than 50% of targeted cyber-attacks last year.[2]

Small businesses are being preyed upon by criminals as 'low hanging fruit'. Having protection for cyber risk is now a fundamental need and smart choice, that is, if it is not already being mandated by business vendor contracts.

With data being so easily lost and stolen (from inside and out), coverage is needed to help a business stay in business. It is not a question of "if" a business will have a data loss but "when".

### *Do small businesses really have an exposure? What happens if they have a data breach without this coverage?*

The exposure is definite, even with encrypted systems and devices. Not even the most secure, large and sophisticated organizations can prevent losses from occurring. When it comes to measuring financial and/or reputational risk, the *Ponemon Institute* data breach studies suggest that over the years, financial losses to businesses are roughly $200 per lost record.[3]

### *What are some examples of cyber claims situations?*

- Malicious hacking of a system shutting down computer systems for an extended period of time resulting in loss of income and extra expenses.
- A disgruntled employee spreads a virus into a computer system destroying data (and backup sources) resulting in expenses to investigate and recreate data.

1. The Denver Post, 2016 60% of small companies that suffer a cyber attack are out of business within six months., 23 (Oct. 2016), available at http://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/
2. Symantec, 2014 Internet Security Threat Report, 6 (Apr. 2014), available at http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_re-port_ITU2014.pdf.
3. Ponemon 2017, Cost of Data Breach Study: Global Analysis, (May 2017), available at https://www.ibm.com/security/data-breach/

- Teenage hacker sabotages data network with Crypto-Locker type malware, and demands an extortion fee of $50,000 to unlock your own data.
- Extortion demands of $25,000 to prevent sensitive customer data from being released on the internet to identity thieves and the general public.
- Lost laptop containing sensitive personal information of customers results in a data breach requiring investigation, notification and credit monitoring expenses.
- Lost patient health information results in regulatory fine.
- Credit card processing encrypted POS payment system has a virus resulting in a credit card data breach. Payment Card Industry (PCI) fines and penalties mount.
- Customer data is breached, class action lawsuit filed. Duty to defend policy responds.

### *What are the actual exposures?*

In addition to protecting their first party exposures, businesses are responsible for the data of others within their control. It doesn't matter how data is lost/stolen (provided it is not the owner of the organization stealing from itself), data risk management tools and insurance protection can help protect the business from the following:

**First Party Expenses**: Data destruction, eBusiness Network Interruption, Cyber Extortion, Breach forensic investigations, Public Relations management, Legal Services, Incident Notifications and Credit Monitoring Services.
**Third Party Liabilities & Expenses**: Legal Liability, Regulatory Fines and Penalties and Payment Card Industry (PCI) Fines and Penalties.

Aon CyberBusinessPro typically ranges between $200 and $2,000 for organizations having less than $10M in gross annual receipts and 50 or less full time employees. Individual pricing varies based on industry, annual gross sales and the limit of coverage chosen.

Given the cyber threat, and the fact that small businesses are routinely targeted, it's important you discuss this exposure and offer a comprehensive cyber insurance program to your small business customers.