GRAMERCY
RISK MANAGEMENT

CYBER RISK ON MAIN STREET

Cyber risk affects any business that uses technology or manages digital information. *Cyber risk* is the possibility of financial loss arising from the information management, IT systems, digital technology and devices – Recovering from an interruption in operations, restoring data, and customer notification and credit monitoring services costs can be substantial.

If you think your business is too small, think again. According to a study conducted by the Ponemon Institute examining cyber security in small and medium-sized businesses, 61-percent of respondents experienced a cyber-attack and 54-percent had data breaches in 2017. Both were increases over 2016. Phishing/social engineering, web-based attacks, general malware and compromised/stolen devices are the most common attacks reported. The negligent act of a contractor or employee, a third-party's mistake or an error in a system or operating process were the main reasons cited for data breaches.

Cyber risk also includes potential damage to a company's reputation. This risk exists for any company that depends on its name or brand to attract (and keep) customers, employees and other stakeholders. Even in a small market a data breach calls into question the ability of a company to protect its customer's private information.

As expected, each industry has different cyber liability exposures based on their operations and how much data they store and manage. In construction, the decentralized nature of the industry requires the use of laptops, iPads and other mobile devices. If not properly secured, they are ripe for data theft and network intrusion. Unlike retail, construction firms do not store credit card information, but they do have intellectual property and other confidential information that is valuable for criminals. The decentralized nature of financial institutions, presence of personal identifiable information (PII) and the large amounts of fund transfers make this one of the most vulnerable industries. In 2018, Marriott International suffered a massive cyber-attack that compromised the personal information of almost one half-billion guests. Hilton, Hyatt and Radisson also experienced cyber losses from data breaches and hacking. The massive amount of electronic personal health information makes long term care facilities especially vulnerable to targeted cyber-attacks. The Internet of Medical Things (Wi-Fi capable medical devices and apps that connect to systems through online networks) extends the exposure.

After identifying vulnerabilities, a company can take several practical steps to reduce its overall exposure.

Check Your State's Data Breach Notification Law

Every state requires businesses to notify and report cyber breaches of PII to affected customers or other individuals. A report to the state attorney general and credit reporting agencies is typically required. A forensic investigation to determine the type and extent of the breach may be needed. Depending on the size, extent and type of breach and data involved, affected people may be entitled to a credit monitoring service, typically for a year. Companies must understand the legal requirements in their state and be able to respond in the event of a data breach, as required.

Train Staff

In the Ponemon study, 54-percent of respondents who experienced a data breach indicated it was due to a negligent employee.   Clicking on a link within a phishing email can release malware into your system.

Update When Prompted

Updates contain changes that fix glitches and enhance the security and performance of software and applications.   Hackers and cyber criminals will search for outdated software to exploit.

Former Employees

Employees should not be able to log into your system or use devices after they leave the company.

Passwords

Require strong passwords – upper- and lower-case letters, numbers and at least one character (comma, percent sign, dash) – and change them periodically.   Use strong PINs or passcodes on mobile devices. Interruptions or loss productivity are poor excuses not to change passwords.

Secure Portable Devices

Adopt a policy that requires staff to secure and safeguard mobile devices when they are used in the field and away from the office.

Adopt Disposal Protocols for Sensitive Documents

Bank receipts, invoices, financial records, medical information and PII should be shredded (to at least level three – 1/16") or sent to a professional shredding and disposal service.   Identity thieves exist off dumpster diving.