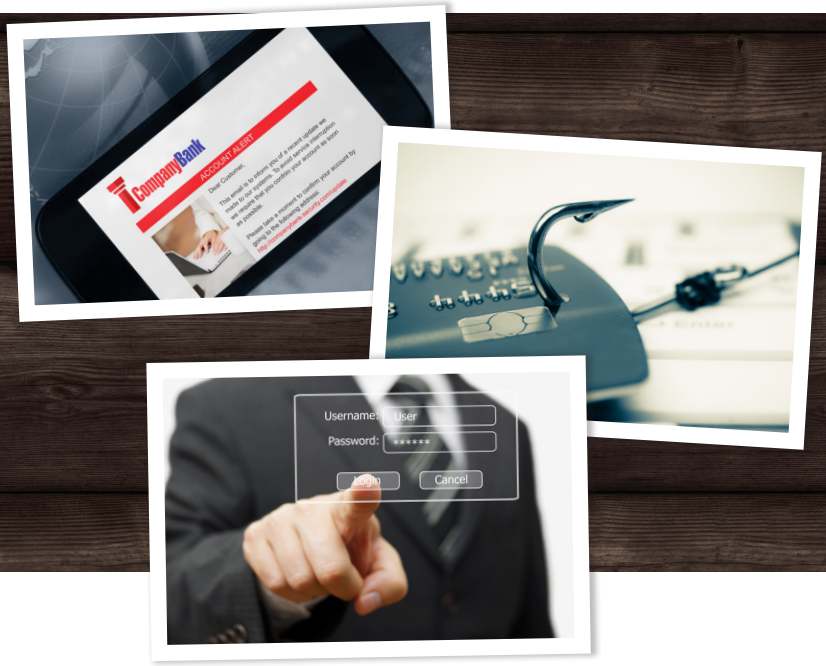
PARKER | SMITH | FEEK

COMMERCIAL INSURANCE
EMPLOYEE BENEFITS
PERSONAL INSURANCE
RISK MANAGEMENT
SURETY



CYBER SECURITY

JUNE 1, 2017

CYBER SECURITY INSURANCE: AN EXPECTED COST OF DOING BUSINESS?

Nicholas Warren | Vice President, Account Executive

Our personal lives continue to move predominately online and the business world has followed suit. Regardless of industry, technology has shifted from a valuable asset that helped make companies more efficient, to a necessary system that now runs the organization. From healthcare, retail, professional services, manufacturing, and those industries in between, protection of company's sensitive information within their technology systems is critical. Management teams across the globe have now created task forces focused on:

- Enterprise Risk Management (ERM)
- Enterprise Resource Planning (ERP)
- Crisis Management/Disaster Recovery
- I.T. services (firewalls, encryption, remote access verification, systems back up, etc.)
- Threat and Vulnerability Assessments
- Cyber security incident response planning

IT'S NOT IF, IT'S WHEN?

Whether it's a Fortune 500 company, a governmental agency, or a beloved Portland microbrewery, companies now must pay attention to hackers, malware, and other causes for breaches of a business' infrastructure. These malicious attacks are seeking sensitive information obtained from customer's online payment methods (PCI), employees/customer personal data (PII), personal health information (PHI), and/or corporate data assets/ intellectual property (IP).

THE HACKERS ARE PATIENT, AND WATCHING.

Last year, while standing in a line on our way home from underwriting meetings, the treasurer of a large, international manufacturing company handed me his phone to read an e-mail titled, "Subject: Urgent." He had retired earlier that summer, and the new CFO had been with the company for less than a week. The "urgent" e-mail was apparently from his new CFO, requesting an urgent wire transfer of $64,500 to a highly valuable vendor for materials required to fill a rush order. Smiling, the treasurer laughed because we had been discussing this issue for the last year during our internal risk strategy discussions.

> [Intruders] watch and learn a company's style of writing, grammar, and wait for the perfect opportunity to strike.

continued >

This incident was obviously a scam, as the treasury department did not handle the wire transfers. This responsibility fell to the financial manager, and we had established protocols earlier that year where two signatures and the original sender's approval were required for wire transfers exceeding $25,000.

Not only can intruders enter organization's protected networks and systems, they watch and learn a company's style of writing, grammar, and wait for the perfect opportunity to strike. Luckily, in this situation, the deception attempt was caught and not rewarded. These situations are becoming more frequent, especially when attackers know management is boarding an airplane, attending a conference, leaving for vacation, or attending similar events that have them distracted.

PROACTIVE VS. REACTIVE

The adage "Plan your Work and Work your Plan" is key. Proactive risk management addressing these cyber security incidents is vital to the financial and operational sustainability of any organization. What if critical infrastructure becomes inaccessible for 8 hours or more? What procedures are in place to fulfill orders, confirm client appointments, or meet critical deadlines while systems are down?

Important risk management strategies to consider include:

1. **Awareness** of these situations and circulating the information internally through employee training, all-staff emails, company intranet announcements, and communication updates.

2. **Empowerment** of staff to raise questions and concerns. These malicious acts are preying on the hierarchical nature of organizations. A low/mid-level staff member trying to impress C-Suite Executives may quickly complete an "urgent" task without question.

3. **Preparation**. Cyber roundtable discussions conducted by senior management on an annual basis are necessary. These roundtables should cover current plans and procedures, implemented changes, items being improved upon, team member responsibilities, and running a simulated cyber event. Within these security exercises, leaders are evaluated on how they handled the mock situations and feedback is provided for improvement.

THERE'S INSURANCE FOR THAT.

Stand-alone cyber liability policies had a slow start towards adoption, but have grown considerably in the last ten years. Since 2010, the policies are now tailored to industries and specific exposures. Cyber liability insurance coverages include:

- Privacy coverage
- Network security
- Media
- First-party coverage
- Cyber extortion
- Errors & omissions

continued >

Additionally, should a suspicious wire transfer not be caught within your established protocols, insurance coverage is available from a commercial crime policy for "deception fraud" or "social engineering." Deductible/retentions vary based on risk exposures, but limits are available up to $5 million. Detailed underwriting and questions regarding controls and risk management practices are required once the coverage limits exceed $500,000.

The 2017 Global Opportunity Report[1] reveals that many companies are not prepared for or understand the cyber risks they face. In fact, only 37 percent of organizations have a cyber incident response plan in place. If you are concerned about how a threat may impact your organization, speak with your commercial insurance broker about best practices and available risk transfer solutions (including legal and defense costs). **Cyber-crimes are becoming more prevalent by the day; don't be unprepared when the target becomes your organization.**

1. http://www.safety4sea.com/wp-content/uploads/2017/01/DNV-GL-Global-Opportunity-Report-2017.pdf