LISA A. BELLIS, ARM, CSM, CIC, CRIS
RISK MANAGER, BROWN & BROWN OF LEHIGH VALLEY, LP

CYBER ATTACKS: THE MOST UNSPOKEN, UNPLANNED FOR, YET COSTLY EXPOSURE

December 2013, Target became the victim of one of the largest data breaches reported in U.S. history. Hackers made away with credit/debit card records for over 40 million customers, along with email and mailing addresses of approximately 70 million customers and vendors. The breach was caused by malware installed on the company's networks, which siphoned customer information during the peak shopping season.[i]

November 2014, North Korean hackers attacked Sony Entertainment over a movie that depicted North Korea in a negative light. Hackers stole private data and released confidential information to the public, leading to the cancellation of "The Interview." Contracts, film budgets, salaries, social security numbers, and even films were stolen.[ii]

February 2015, Uber's data was accessed by an unauthorized party, compromising approximately 50,000 Uber drivers' names and license numbers across the United States.[iii]

March 2015, Premera Blue Cross became a victim to a cyber attack which exposed both the medical and financial information, including: clinical records, bank account numbers, social security numbers, and birth dates of 11 million people.[iv]

November 2016, the United States readies itself against potential foreign hackers who are trying to undermine the 2016 United States Presidential Election. In response, the U.S. Department of Homeland Security, the CIA, National Security Agency, and other governmental agencies have mounted an unprecedented effort to counter these potential attacks.[v]

Think it can't happen to you? Think again! Here are the top three reasons why business owners feel it will never happen to them…

1. ***My business is too small, which makes us unappealing to hackers***. Although news headlines depict large retailers, banks, and other large companies as victims of cyber attacks, small business owners are susceptible to attacks as well. These smaller businesses typically accept credit card payments, and maintain personal information about their customers. Many of these businesses conduct banking online. All of these activities make them an attractive target.

2. ***Our company uses the cloud and the vendor is responsible for handling any interference by a hacker.*** The cloud is nothing more than someone else's computer and is just as vulnerable to a cyber attack. While the vendor will have responsibilities, the user has the highest level of responsibility to ensure they are maintaining data security on those systems. The user is also responsible for notifying affected parties of any suspected breach.

3. ***If an attack occurs, we'll just handle it.*** The overwhelming majority of businesses that suffered an attack do NOT survive! The average cost to restore just one file is over $154. Multiply that by all of your customers and it adds up fast!

Here are the latest statistics involving cyber breaches:

- ✓ Over 500,000,000 personal records were stolen or lost in 2015.[vi]
- ✓ Small businesses (250 or fewer employees) were the target of 43% of spear-phishing attacks in 2015.[vii]

- ✓ The average direct costs of a security breach on small businesses are $38,000, according to a study from Kaspersky Lab. This includes downtime, lost business opportunities and professional services to mitigate the breach. Research shows, on average, small businesses can expect to pay $10,000 in professional fees, including: IT security consultants, risk management consultants, lawyers, auditors, accountants, and public relations consultants.[viii]

- ✓ The projected cost of cyberattacks in 2019 will reach approximately $2.1 trillion. [ix]

What is the financial impact to an organization? Let's break it down into two categories: First Party damages, which includes damages an organization directly incurs and Third Party damages, which include damages resulting from third parties affected by the breach.

First Party Damages
- ✓ Legal Expenses
- ✓ Notification Expenses
- ✓ Public Relations
- ✓ Data Loss
- ✓ Credit Monitoring For Customers
- ✓ Business Interruption and Extra Expense
- ✓ Forensic Investigation of the Breach

Third Party Damages
- ✓ Legal Defense
- ✓ Settlements, Judgments, and Damages Awarded
- ✓ Cost to Reimburse Banks for Re-issuing Credit Cards
- ✓ Regulatory Investigation Expense

The average cost paid by organizations for each lost or stolen record has increased to $154 in the 2015 study by IBM and Ponemon Institute. Lost business caused by damaged reputation may have the most severe financial impact on businesses. To compound matters, the average time it takes a business identify a breach can be over 256 days. Statistically, the longer the breach goes unnoticed, the more severe the financial impact on the business. The good news is there are ways to prevent or reduce the effects of cyber attacks, including:

- ✓ **Identify Your Exposures:** By analyzing your technology, people and processes, you will gain a clearer picture of potential holes in your security. Review and modify your plan regularly, because new risks arise often, sometimes even daily!

- ✓ **Invest in Cyber Security:** While none of these companies claim they can totally eliminate cyber attacks, they detect breaches early enough to minimize the financial impact of an attack on an organization. Firms such as Norton, CISCO, RSA, McAfee offer cyber security services.

- ✓ **Conduct Frequent and Regular Software Updates:** Ensure your IT department frequently and regularly install and update security patches to your devices' operating software.

- ✓ **Encrypt Sensitive Data:** If the theft of a mobile device or portable laptop presents a possible data breach, then consider encrypting sensitive data. This is considered a last line of defense. When data is encrypted, even if it's stolen, it cannot be used. As well, unencrypted devices are often not covered by a cyber liability policy, so make sure you know whether you need to encrypt your devices or not.

- ✓ **Enforce a Strict Password Policy:** Although this procedure is typically not a favorite with employees, it is vital in order to reduce cyber liability risks. Require password updates monthly. Encourage employees to use different passwords for different systems.

- ✓ **Implement BYOD Policies & Procedures:** This written policy should include instructions concerning the type of data that may be accessed on personal devices, as well as procedures for securely accessing, transmitting, and storing information. One resource, offered through AT&T Toggle, allows employees to switch from "work mode" to "personal mode" on their smartphones. Make sure the policy is clearly communicated to all employees.

- ✓ **Provide Staff with Data Security Training:** Ensure this training is incorporated into the new hire orientation process and to all employees throughout the organization regularly. Human error is a significant factor contributing to cyber liability exposure. Topics that an organization should consider covering may include: BYOD (bring your own device) policies, network security procedures, encryption instructions, data breach notification laws, and the impact of cyber liability claims to the organization. Your organization may also include educating employees about phishing and pharming scams. Remind them not to click on anything that looks suspicious or seems too good to be true.

- ✓ **Know Your State's Notification Requirements:** Each state has different notification requirements, including how the notification is to be issued and the time-frame for notifying affected parties. To learn more about your notification responsibilities, visit http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

- ✓ **Protect Your Organization Through Cyber Liability Insurance:** This insurance is specifically designed to respond to the risks associated with cyber liability. Be sure to speak with your broker to make sure you design a coverage plan that meets your needs. Beware of exclusions, sub-limits, and requirements such as encryption!

Despite the best efforts and intentions, breaches in security do occur. Should your organization experience a data breach, you will need to be prepared to quickly respond by following your Crisis Management & Response Plan. The first step is determining when and how the breach occurred, what information was accessed, and how many individuals were or may be affected. Keep your customers informed on the actions your company is taking and utilize PR firms to restore or maintain your company's reputation.

---

[i] The New York Times, Kevin Granville, February 5, 2015, "9 Recent Cyberattacks Against Big Businesses"
[ii] Vox, Timothy B. Lee, December 17, 2014, "The Sony Hack: How It Happened, Who Is Responsible, and What We've Learned"
[iii] The Daily Dot, Dell Cameron, February 27, 2015, 11:34 PM, "50,000 Uber Drivers Compromised in Newly Reported Cyberattack"
[iv] The Huffington Post, Jim Finkle, March 17, 2015, "Premera Blue Cross Hacked, Medical Information of 11 Million Customers Exposed"
[v] NBC News, Nov. 3, 2016, 10:12 PM ET, Exclusive: "White House Readies to Fight Election Day Cyber Mayhem"
[vi] Softpedia, Catalin Cimpanu, April 12, 2016 17:10 GMT, "Over Half a Billion Personal Records Were Stolen or Lost in 2015"
[vii] Insights, Fran Howarth, "Spear-Phishing Attacks Increased by 55 Percent in 2015"
[viii] Business News Daily, Chad Brooks, October 12, 2015, "Worried About a Cyberattack? What It Could Cost Your Small Business"
[ix] May 12, 2015, http://www.securitymagazine.com/articles/86352-cybercrime-will-cost-businesses-2-trillion-by-2019, "Cybercrime will Cost Businesses $2 Trillion by 2019."