

INsight

MARCH, 2010

Keeping Technology Risks In Check

with **Scott Schleicher**, AVP, Manager—Technology E&O
and **Steven Anderson**, AVP, Senior Underwriter—Select Professional

IT'S A TECHNOLOGICALLY DRIVEN WORLD. FROM LAPTOPS TO PERSONAL DIGITAL Assistants (PDAs), from memory sticks to web servers, all kinds of technology allow us to conduct business anywhere in the world and no matter where we are or where we may go.

Unfortunately, as businesses' reliance on technology continues to grow, vulnerability to cyber risks is growing in tandem. Breaches in computer networks can pose a threat to financial, customer, employee and other proprietary data, putting it in the wrong hands. Hackers can take down a website and totally interrupt a company's online operation. The wrong post on a company website can leave it fighting copyright infringement.

Despite the potentially costly issues that technology poses, far too many companies are overlooking their cyber liabilities. According to the recently released 2009 National Small Business Cyber Security Study, although small businesses today are handling valuable information — storing customer data, financial records, credit card information, intellectual property and other sensitive corporate content online — few have cyber security policies to ensure the safety of their employees, intellectual property and customer data. Co-sponsored by the National Cyber Security Alliance (NCSA) and Symantec, the study surveyed nearly 1,500 small businesses across the United States. Only 28 percent of U.S. small businesses have formal Internet security policies and just 35 percent provide any training to employees about Internet safety and security.



SIZE DOESN'T MATTER

There is no shortage of privacy breach incidents in the news and companies of all sizes are finding themselves and their customers victim of cyber breaches. One very well known case is that of the TJX Companies, Inc., parent company to TJ Maxx, HomeGoods, Marshalls and other retailers. The company suffered the loss of more than 45 million credit and debit card numbers that were stolen from its IT systems over an 18-month period. The breach reportedly cost the company \$17 million.

More recently, the National Archives and Record Administration lost an unencrypted hard drive containing the detailed records of 76 million veterans and millions of Social Security numbers. For Chicago-based Blue Cross and Blue Shield Association, when an employee allegedly downloaded information about 800,000 doctors on a personal laptop and then lost it, it became a problem. Cheers Liquor Mart, a southern Colorado liquor retailer, went back to basics, returning to paper receipts and dial up credit card approvals, when it discovered that its wireless broadband system was hacked and customers' debit and credit card information was stolen.

According to a recent study by McAfee, mid-size businesses, those with employees from 51-1000 employees, have seen an increase in security breaches over the last year. The survey of



900 mid-size businesses found that over the last year, one of five of them were estimated to have lost \$41,000 in sales on average as a result of a security breach. More than 70 percent of respondents believed that a serious security breach could put them out of business. Ironically, during the current recession, these statistics are unveiled at a time when most company's IT budgets have dropped and companies are even looking at ways to cut expenses in their security measures.

Another result of the current economy may also be the increased threat of extortion. A disgruntled or rogue employee can do a lot of damage with valuable information. For instance, a laid-off IT administrator was recently arrested and faces up to five years in prison after he tried to extort money from his former employer, a NY-based mutual fund company, by threatening to crash the company's servers. Demanding a better severance package, he threatened to use his connections with hackers in Eastern Europe to wreck havoc on their customers' private information. This is a particularly popular tactic emerging from Eastern European invaders who threaten

to post proprietary information — an employee list with private information, for example — if a company doesn't pay ransom or an asking price.

Technology-related risks can cost a company plenty, especially in cases like these where customer or employee information is compromised. First, companies conducting business in the United States must manage myriad changing privacy regulations which often require them to immediately disclose, usually in writing, to their customers any breaches of personal information. The costs associated with notifying customers about breaches can be substantial. According to Ponemon Institute's *Fourth Annual Cost of Data Breach Study*, the average cost of a data breach is \$202 per customer record. Additionally, businesses may also find themselves paying for costs related to crisis management efforts, restoration or reconstruction of data and may also be susceptible to potential third-party claims — general damages, out-of-pocket expenses related to data restoration or credit monitoring services for those affected by a privacy breach.

MORE THAN FIREWALLS

So how does a company protect itself from cyber risks? In general, risk management is not about being reactionary, but proactive. Companies need to recognize that they have tremendous risk to identity and security breaches and are closely examining their risk management strategies, including employee training and insurance, to reduce their exposure.

Looking at ways to prevent a potential loss is always a good first step. For instance, to minimize their potential privacy liability, companies are wise to:

- Train employees and contractors to understand their responsibility in the protection of data assets.
- Ensure that mobile devices are encrypted and that employees understand the organizations' policies with respect to downloading sensitive information and working remotely.
- Make employees aware of the precautions that should be taken when traveling with laptops, PDAs and other data bearing devices.


Additionally, there are technology insurance policies available today that help protect commercial businesses from a variety of tech-related liabilities. While cyberliability insurance has been around

in some form or another for the last decade, insurers have carefully expanded the insurance protection they offer. With underwriters who have worked in the technology industry and are aware of the risks that technology poses, insurers have extended their coverages to include a wide range of cyberliability coverage under one policy form, including:

- Network Security Liability
- Media Content Services Liability
- Privacy Liability
- Extortion Threat
- Crisis Management
- Business Interruption
- Credit Monitoring
- Privacy Notification Costs
- Regulatory Fines
- Technology Errors & Omissions (E&O)

A company may feel more secure with all of these coverages or just a few — depending on the nature of business and the breadth of information stored in your computer systems. For example, a web-hosting company with its vast amount of private information on numerous companies may seek more extensive protection including technology E&O to address professional liability exposures to the services it renders. On the other hand, a retailer, with all its customer information including credit card numbers, might want benefit most from the crisis management,

credit monitoring and privacy notification costs that this insurance protection affords. A company's tech insurance can be very tailored to address its specific insurance needs based on its technology usage.

In the whole scheme of things, cyber insurance policies may be very inexpensive when compared to the potentially enormous costs associated with any kind of data breach. Especially as the world becomes ever more interconnected and dependent on networks, laptops and personal handheld devices, protecting information and privacy is going to be a big risk management challenge for all industries. 

Scott Schleicher is AVP, Manager – Technology E&O and Steven Anderson is AVP, Senior Underwriter in the Select Professional unit of XL Insurance.

More information about XL Insurance's technology products visit

<http://www.xlinsurance.com/xltech>.



INsight is an XL Insurance publication. Copyright 2010. All rights reserved. "XL Insurance" is a registered trademark of XL Capital Ltd and the global brand used by its insurance company subsidiaries. In the US, the XL Insurance companies are: Greenwich Insurance Company, Indian Harbor Insurance

Company, XL Insurance America, Inc., XL Insurance Company of New York, Inc., XL Select Insurance Company, and XL Specialty Insurance Company. In Canada, coverages are underwritten by XL Insurance Company Limited-Canadian Branch. Not all of the insurers do business in all jurisdictions nor is coverage available in all jurisdictions.

If you have any feedback or suggestions on INsight, please contact Sarah German, Vice President, Marketing & Communications, Americas. Sarah.German@xlgroup.com. 505 Eagleview Blvd, PO Box 636, Exton, PA 19341 • 888-609-2518 • 800-327-1414 • www.xlinsurance.com