CYBER LIABILITY:
How to Grapple with Continuously Evolving Risk

Businesses battle new threats daily thanks to social media, mobility, the cloud and other technologies, but preparation and risk transfer can help you confront cyber-attacks when—not if—they occur

By John W. DeWitt

New online publishing and social media venues. New applications and business systems. New, and almost always mobile, devices. And with the cloud, new locations for your data and applications, from around the corner to around the world. Technological change maintains its relentless pace—and each new development brings new risk factors that businesses ignore at their peril.

It's no longer a question of "if," but rather, "when," a cyber-related threat confronts your business or your clients' businesses, warned Laura Toops, editor of *American Agent & Broker*, as she kicked off a recent PropertyCasualty360 web seminar titled "Cyber Liability: A View from the Trenches." Citing Ponemon Institute data, Toops noted that 71% of businesses surveyed faced cyber-attacks in 2011. Yet the majority of companies remain unprepared for cyber-attacks that can threaten their data, their customers' data, their employees, and the operations and reputation of their businesses, Toops said. Only 38 percent say they are increasing their 2012 budgets to address these cyber threats.

EVERYONE'S ON THE HOT SEAT

All too often, cyber liability still is viewed as a problem to be addressed by the IT department. That's a critical mistake, Toops said, because a cyber-attack puts "a lot of people on the hot seat"—among them agents and brokers, risk managers, senior management, outside auditors, and even a company's board of directors. She cited the recent example of Wynham; in June, the Federal Trade Commission sued the hotelier for alleged data security failures that resulted in three security breaches during the past two years.

Remarkably, only a third of companies today have cyber-related insurance coverage. "The question is, 'Why not more?'" commented attorney Lori S. Nugent, co-chair of the data security and cyber liability practice at Wilson Elser, as she shared her experiences helping clients cope with real-world cyber losses and the litigation that frequently follows cyber-attacks. "Both individuals and the companies they work for can be sued."

Nugent delved into a number of risks associated with the rise of e-publishing and social media—in particular, the risks associated with defamatory communication. It can be easy to forget in the effortlessness of online commentary that "if you say something defamatory, you can be sued," she said. Prior to the Internet age, damages from defamation cases were often linked to the circulation of a publication. "Now, it can go viral and literally go around the world." Online endorsement or disparagement of products—whether your own company's products or a competitor's—also is risky ground, Nugent added—especially "in cases of failure to disclose that you work for the company."

TRACKING FOR TROUBLE

Privacy violations are another critical concern for companies—especially with the widespread use of technology to track web site visitors. Tracking of visitors to your company's web site can be fodder for class action lawsuits, according to Nugent, especially "when individuals visiting your site didn't authorize the tracking and you're using technology to track everywhere the user goes even after they leave your web site." On the other hand, she said, "we've had good success in litigation when our clients could prove that either they didn't track or that the tracking was approved by users."

Unfortunately, "sometimes companies are not aware of the tracking that is being done on their behalf," Nugent warned. For example, this can happen when, unbeknownst to the IT or legal departments, a third-party vendor convinces the marketing department to implement tracking to gather more useful data on web site visitors. It is crucial that companies "know what tracking vendors do in your name," she said. Companies should make a clear decision—either to not track their web site users, or to track very carefully, with clear consent from users.

RISK TRANSFER FOR CYBER LIABILITY

Cyber insurance represents another key way to prepare for the threat of cyber-attack. But companies must do their homework to figuring out what coverage to pursue—and how their risk management efforts can translate into lower costs for risk transfer solutions.

Going through the application process is an important first step, said Scott Hammesfahr, who specializes in cyber liability underwriting for Zurich North America. Completing an application serves three main goals. First, it facilitates communication between departments that may not work together regularly such as IT, HR, Legal, and Risk Management. Second, it will set pricing expectations for risk transfer solutions allowing for better budgeting. Finally, it highlights the sorts of controls that underwriters feel most contribute to effective risk management. Underwriters and agents often can provide guidance on where the company should improve cyber risk management—including recommending third-party technical consultants to implement better controls that in turn can reduce the cost of transferring cyber risk.

People, processes, and technology are all important factors in the underwriting of cyber risk coverage, Hammesfahr explained. Companies should have qualified employees with clear accountability for data security and privacy, training should be formalized, and efforts must be coordinated across internal departments. Formal processes should encompass security and privacy policies, regulatory compliance, disaster recovery planning, network mapping, password management, physical records, and more. Technology should "establish the front line of defense with the right technology security tools and products such as firewalls, encryption, monitoring tools, and established redundancies," he said.

Cyber risk transfer solutions vary by carrier, so companies seeking to purchase cyber insurance coverage should pay close attention to what is covered, Hammesfahr said.

KEY QUESTIONS TO ASK INCLUDE:

- Does coverage extend to third-party service providers?
- Is there coverage for the actions of rogue employees?
- Are there sub-limits built into the coverage form?
- Does privacy breach coverage apply regardless of applicable notice laws?

PREVENTING AND MITIGATING CYBER LOSSES

Data breaches—not just hackers breaking into networks, but especially the loss or theft of devices and paper-based data—remain a company's most commonplace cyber risk. Nugent prescribed several key steps for protecting businesses:

1. **Moderate your data diet.** Take in only the information you need, discard it when you don't need it, and never share it unless the other party needs it and you are authorized to provide it.
2. **Protect sensitive data.** Physical security remains very important—so lock your cabinets and office doors. Implement robust firewalls, encryption, and other forms of network security. Protect mobile devices used by employees with encryption, the ability to remotely "wipe" the device if it's lost or stolen, and ideally by not allowing sensitive data to be loaded onto the device in the first place.
3. **Have a written security plan.** An information security plan should document what sensitive information you handle—what you receive, what you keep, and what you send—how you protect it, and what you do in case of a breach.
4. **Have a breach response plan.** Eliminate finger-pointing by knowing who is responsible for what, when must notification be provided, and who must be notified. Take steps to ensure regulator and contractual compliance. Recognize that nothing is "off the record" and that it takes effective response to protect your reputation and your business.

John W. DeWitt, an event moderator and contributing editor for National Underwriter Property & Casualty, *PropertyCasualty360,* American Agent & Broker, *and other insurance industry publications, is principal and senior consultant for JW DeWitt Business Communications in New Salem, Mass.*