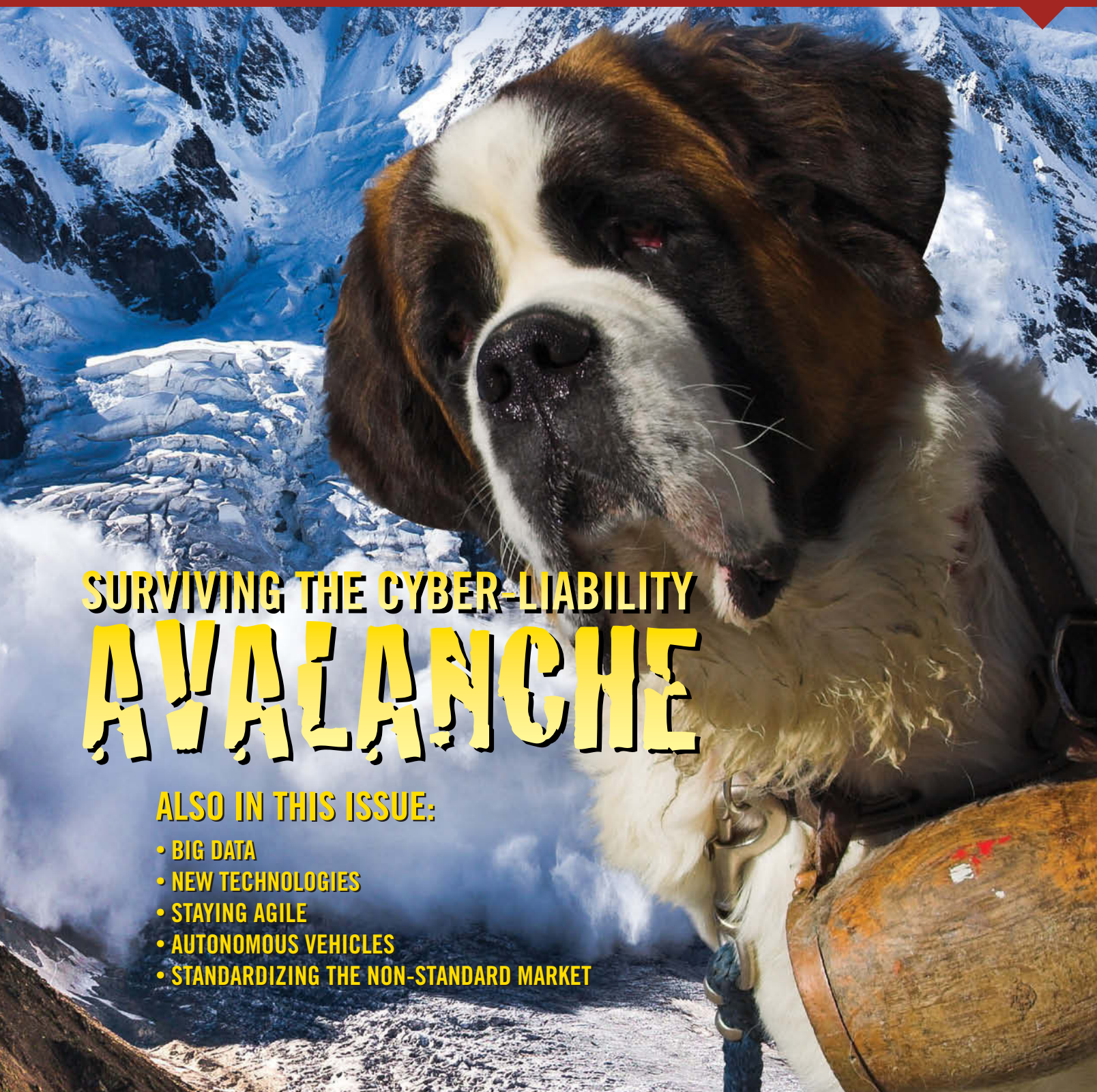
WIN

WHOLESALE INSURANCE NEWS

A Publication of the
AAMGA
American Association of Managing General Agents

SPRING 2016
VOLUME 5 | ISSUE 4

INFORMATION EXCLUSIVELY FOR THE WHOLESALE INSURANCE PROFESSIONAL



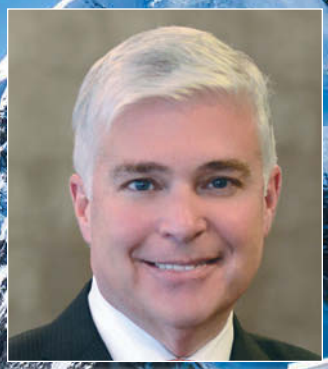
SURVIVING THE CYBER-LIABILITY AVALANCHE

ALSO IN THIS ISSUE:

- BIG DATA
- NEW TECHNOLOGIES
- STAYING AGILE
- AUTONOMOUS VEHICLES
- STANDARDIZING THE NON-STANDARD MARKET

SURVIVING THE CYBER-LIABILITY AVALANCHE:

HOW CONTRACTS WITH BUSINESS PARTNERS AND VENDORS EXPOSE COMPANIES TO CYBER-LIABILITY



BY THEODORE M. SCHAER AND ELIZABETH S. FITCH

RECENT HIGH PROFILE data breaches are indicative of the cyber breach avalanche that has arrived. For every Target, Sony, and Anthem, there are dozens of small to mid-size companies that are data breach victims. The 2015 McAfee Security Paradox Report reveals that 63 percent of midsize U.S. companies (51 to 1000 employees) have experienced a data breach this year.[1] And why? The answer is simple: Small to mid-size businesses lack proper security and administrative controls, thus making them easy targets for hackers. According to a Symanteck report, 50 percent of the cyber attacks were directed at businesses with less than 2,500 employees with the largest segment being companies with less than 250 employees. A report by PWC indicated that 10 percent of organizations that suffered a breach in the last year were so damaged that they needed to change the nature of their businesses completely.

Companies that maintain Personal Identifiable Information (PII) and contracts with outside vendors and business partners are particularly vulnerable. In many cases, vendors were the weakest link in the security chain, and thus to blame for the entire breach. The 2013 Trustwave Global Security Report indicated that over half of security breaches surveyed were linked to a third-party vendor. The Department of Veterans Affairs' breach was due to a security flaw in one of its home Telehealth vendors. Target's breach was suspected to have come from their HVAC vendor.

Despite vendors being the cyber breach culprit, the company bears the loss and expense of the breach. This is because companies have not been proactive in vetting vendors, negotiating contractual provisions, and obtaining the proper insurance coverage. Where there is risk there is also opportunity. Not only does a company need to minimize cyber risk by properly vetting vendors, but also can shift the risk to its vendors through well drafted service contracts and insurance requirements.

VENDOR SERVICE AGREEMENTS

Many companies elect to outsource operational functions to outside vendors. While vital to profitability, it can create additional cyber risks. Vendors do not have to control a company's data to create a weak link in the security. Even data processors, who hold or process personal data for a company, but are not responsible for the information, could be the access point for a breach. Failure to properly vet a vendor's cyber capabilities could be a costly omission. Requiring a vendor to submit to a risk assessment audit would be the best way to protect against cyber exposure but that is not a practical or economical solution for most small to mid-sized companies. Simple and inexpensive vetting practices can be implemented. Before engaging a vendor it is important to understand the cyber security controls that the vendor has in place. Have the vendor fill out a security questionnaire that addresses the following:

1. Data security technical and environmental controls;
2. Data collection, retention and destruction policies;
3. Privacy policies and compliance with applicable regulations;
4. Breach incident response plan;
5. Employee training;
6. Complaints about handling of PII.

The responses will be telling. Selecting a vendor that has well defined policies and practices will reduce cyber exposure.

Mid-size companies have the bargaining power to mandate vendor compliance with cyber policies that minimize risk. Before hiring any outside vendor, a company should provide the vendor with written expectations for regulatory and data security policy compliance and secure a warranty from the vendor that it has the technical and administrative capacity to comply.

Once the outside vendor has been selected, outsourcing provides the opportunity to shift the risk of cyber from the company to the vendor. The service contract should not only incorporate the express warranty elicited during the selection process, but should also include specific provisions designed to shift risk of a cyber breach to the vendor.

CONTRACTUAL INDEMNIFICATION

The written contract that your business enters into with vendors sets forth the understanding of each party regarding the deal. Typical contract terms include consideration exchanged, time for performance and remedy in the event of a breach of the agreement. Contractual indemnification clauses are routinely inserted into contracts to spell out who is responsible for unintended losses arising from the performance of the contract. These provisions are common in many industries and typically have been enforceable. A well drafted contractual indemnification provision that imposes the duty to defend and indemnify on the service provider shifts the cost of defending a third party claim from the company to the service provider.

A COMMON PITFALL OCCURS WHEN AN INDEMNIFICATION OR LIABILITY CAP IS ADDED TO AN EXISTING SERVICE AGREEMENT. AMENDING THE SERVICE CONTRACT TO INCORPORATE INDEMNITY OR LIABILITY CAPS CAN CREATE CONFLICTING AND/OR CONTRADICTORY TERMS THAT INVARIABLY LEAD TO ADDITIONAL LIABILITY AND HIGHER COSTS.

A common pitfall occurs when an indemnification or liability cap is added to an existing service agreement. Amending the service contract to incorporate indemnity or liability caps can create conflicting and/or contradictory terms that invariably lead to additional liability and higher costs. Another pitfall in contract drafting is defining terms. Many contracts attempt to define the scope of damages but leave the damages-related-terms too vague or too specific. Damages that are defined too specifically could leave companies open to unintended risk. Any term that is vague or ambiguous will need a court to define it, requiring even more litigation to add to mounting legal costs. Indemnification clauses are generally broad and encompassing. It is recommended that in the cyber space, these clauses be tailored and specifically apply to a data breach particularly if the outside vendor is not in the data processing or data security business. Clauses which are specific as to the type of damages being indemnified will strengthen your position to recover from harm in the event of a breach.

The flip side is that vendors will include boiler plate reverse indemnification and limitation of liability provisions in their service contracts. These boilerplate provisions are enforceable in most jurisdictions

so a careful review of the service provider agreement is critical to risk assessment and risk transfer. One pitfall is that companies allow their IT managers to review any vendor service agreement concerning digital information storage or process. Though capable in their field, IT managers review for security parameters and do not focus on legal issues of indemnification or warranty waiver language in relation to a data breach. This causes the agreements to lack specific clauses that offer additional protection and minimize risk. The better approach is to have legal counsel carefully evaluate and negotiate of indemnification provisions. Indeed, each jurisdiction has unique laws governing the interpretation and enforcement of indemnity provisions. To ensure the company is fully protected from third-party claims, it is imperative that legal counsel review each of the state's breach notification laws and statutory and case law governing the interpretation of risk shifting contract provisions.

ONE PITFALL IS THAT COMPANIES ALLOW THEIR IT MANAGERS TO REVIEW ANY VENDOR SERVICE AGREEMENT CONCERNING DIGITAL INFORMATION STORAGE OR PROCESS. THOUGH CAPABLE IN THEIR FIELD, IT MANAGERS REVIEW FOR SECURITY PARAMETERS AND DO NOT FOCUS ON LEGAL ISSUES OF INDEMNIFICATION OR WARRANTY WAIVER LANGUAGE IN RELATION TO A DATA BREACH.

INSURANCE REQUIREMENTS

Requiring the vendor to procure cyber insurance is one of the best ways to mitigate the significant financial risk associated with cyber exposures. The service contract should include an insurance provision that not only requires the service provider to procure cyber-liability insurance but also requires that the company be named as an additional insured. Traditional business insurance products may not adequately cover losses for a data breach. According to Lemme Insurance Group, the insurance industry has responded by developing Cyber Insurance policies that provide coverage to eliminate or mitigate against the following exposures:[2]

1. **Reputational Risk:** A publicized data breach can result in the loss of reputation in an instant.
2. **Data Corruption or Loss:** Loss, destruction or corruption of data can interrupt not only the day to day operations of a company but also exposes the company to third party claims.
3. **Cyber Crime:** Cyber-criminals prey upon companies that lack sophisticated technological controls and focus on discovering the vulnerabilities.
4. **Technology failures:** Any type of cyber attack — from hacking to malware — can corrupt data and can cause hardware failures resulting in business disruption.
5. **Regulatory Exposures:** Federal Regulators and State Attorney Generals are taking an active role in ensuring that breach notifications laws are followed. Costs associated with defending a regulatory action and the assessment of fines and penalties can be in the millions.
6. **Crisis Management:** Due to the timing requirements of data breach notification laws, a data breach of any kind is a true crisis which requires an immediate commitment of financial and human resources. The cost of notifying customers, regulatory compliance, cooperating with law enforcement investigations and coordinating with credit reporting agencies results are significant.
7. **Website Exposure:** Sources of potential liability for websites include defamation, intellectual property infringement, and negligent misrepresentation.
8. **Third Party privacy claims:** The inadvertent loss or dissemination of personal information data subjects companies to third party claims. Individual and class action lawsuits may very well be the next wave of civil litigation.

The insurance requirements should be very specific and tailored to the company's operational risks and goals. The company can dictate to its vendors the scope of coverage and policy limits. Companies must beware of sub limit traps within insurance policies. Sub limits are pre-set limitations on an amount of coverage available to cover a specific loss. Sub limits are dangerous as they can leave a business that relies on outside vendors exposed by permitting an insurance company to limit certain areas of coverage from specific types of third party vendor claims. Before the vendor is given access to the company's PII, a careful review of the vendor's cyber insurance policy should be undertaken to ensure the vendor procured the proper coverage with sufficient policy limits.

Coverage under the vendor's insurance policy may still leave coverage gaps between a company's cyber risk policy and where their vendor's liability and insurance coverage begins. Companies should require certified copies of insurance policies from all vendors to maintain awareness that there is sufficient coverage and of calendar renewal dates to ensure coverage stays in effect. Be wary when coverage is moved to another liability carrier and demand "tail" coverage for claims that the prior carrier may seek to avoid covering.

BREACH RESPONSE ALLOCATION PROVISIONS

Most current service contracts do not allocate responsibilities for a data breach response between the vendor and company. Depending upon the magnitude of the breach this failure can lead to dire financial consequence. In an average data breach, 28,765 records are stolen or lost. The average cost of each stolen

record ranges from $188 to $246 for U.S. companies.

For general data processor vendors, the service contract should specify what breach response costs will be absorbed by the vendor. For IT vendors that are responsible for maintaining the company's cyber security, the onus should be placed on the vendor to either perform at no cost or pay for the forensic investigation to determine the source of the breach and remedy the breach.

CONCLUSION

Regardless of size, companies are likely to have service agreements with at least a few vendors, each of which can have multiple pitfalls that leave the business exposed. Whether vendors or other business partners are the cause of the breach or seek to bring claims themselves, companies must take action to prevent runaway costs. It is important to take the necessary steps to safeguard the company and limit the amount of liability from these vendors and business partners by carefully reviewing vendor agreements, service contracts and insurance agreements with knowledgeable legal counsel working in conjunction with IT experts.

Theodore M. Schaer of Zarwin, Baum, Devito, Kaplan, Schaer, Toddy, P.C., is Chairman of the firm's Casualty Defense and Cyber-Liability, Privacy and Data Security Departments. Ted has been certified by the International Association of Privacy Professionals. The CIPP/US certification is the preeminent privacy credential in the US private sector. Ted also serves as Chief Information Security Officer for his law firm. Ted counsels companies on cyber-liability and data protection in addition to leading the data breach response team. Ted regularly blogs on cyber-liability issues and has been interviewed by national media on cyber security issues. He can be reached at tmschaer@zarwin.com.

Elizabeth S. Fitch is a founding and managing member of the Righi Fitch Law Group. She is a trial lawyer with 30 years of civil defense experience and has the AV Preeminent rating. Her practice has concentrated on representing businesses and individuals in complex civil litigation matters. She has developed expertise in risk management and assists clients with risk transfer strategies. Beth is board certified in Privacy and US Data Protection (CIPP/US) and serves as the co-chair of the Arizona State Bar Law Firm Data Security, Privacy and Cyber-Liability committee. She represents clients on privacy and cyber related issues and leads her firm's data breach response team. She can be reached at beth@righilaw.com.

FOOTNOTES

1 2015 *McAfee Security Paradox Report, available on line at* http://www.outlookseries.com/N2/Security/4612_McAfee_Security_Paradox_Midsize_Company_Lost_$43K_Breaches.htm

2 Kelly S. Geary, *Cyber Related Business Risks and the Cyber Insurance Solution*, 2014, http://www.lemme.com/assets/1/13/Cyber_Related_Business_Risks_and_the_Cyber_Insurance_Solutions.pdf.