Practical Cyber Law: Why the Standard of Care Requires Lawyers to Have a Basic Understanding of Cyber Insurance

By Shawn Tuma & Katti Smith

Data breaches have become far more common than most people realize. Contrary to common belief, they are not always caused by sophisticated cyber criminals. In fact, most data breaches are the result of far more common occurrences that businesses encounter on a regular basis. For example, each the following ordinary events constitute a security incident:

- A password-protected (but unencrypted) laptop computer is stolen from a company's office, which laptop contained sensitive personal information and financial information for the company's customers.[1]
- An employee goes to a local printing shop, to print a personal document from a USB thumb drive, that also contains unencrypted patient data from his employer, and temporarily leaves it there.[2]
- An employee of a financial institution views customers' account information, containing sensitive personal information and financial information, without having the requisite authority to view such accounts.[3]
- A certified public accountant's external hard drives containing unencrypted sensitive personal information and financial information for his clients and their relatives are stolen from his residence.[4]

---

[1] Heartland Payment Systems Security Breach Notification, State of California Department of Justice, Office of the Attorney General, *at* https://oag.ca.gov/system/files/Heartland%20Payment%20Systems%20Ad%20r1fin_0.pdf? (last visited Aug. 15, 2015).

[2] HIPAA Security Breach Notification, Denton County Health Department, *at* http://dentoncounty.com/~/media/Departments/Health-Services/Health-Department/PDFs/Press_Release_HIPAA%20Breach%20Notification_20150410.pdf (last visited Aug. 15, 2015).

[3] Employee Viewing Information Without Authorization Triggers Data Breach Obligation for Credit Union, Business Cyber Risk Law Blog, *at* http://shawnetuma.com/2015/08/13/employee-viewing-information-without-authorization-triggers-data-breach-notification-obligation-for-credit-union/ (last visited Aug. 15, 2015).

[4] Richard Berger CPA Security Breach Notification, State of California Department of Justice, Office of the Attorney General, *at*

Both experience and research confirm that the greatest risk to a company comes from a failure of basic cybersecurity blocking and tackling. A company is much more likely to experience a data breach by something simple, such as employee negligence, a lost or stolen device, or falling for a social engineering scheme than it is to be the victim of a sophisticated cyber attack.[5] And, these common vulnerabilities are resulting in breaches all the time.

Potential risks vary across industry; however, industry-leading Ponemon's Fifth Annual Survey shows the magnitude of the evolving cyber risk in the healthcare industry alone (*i.e.*, every small, medium, and large provider you know): "Over the past two years, 91 percent of healthcare organizations reported at least one breach, 39 percent reported two to five data breaches, and 40 percent had more than five data breaches."[6] The severe impact these breaches have had and the notoriety they have gained are compelling examples of why we must understand the risks so we can understand how to advise clients about how to protect their business from this type of loss.

The pressure to understand cyber risk crosses all industry boundaries because almost all but the most primitive of today's businesses conduct ecommerce. Consider how many businesses you know that do not (1) use a computer, (2) receive, store, or transmit electronic data, or (3) connect to the Internet. Unless such a business does not do any of these things, it is at risk of vulnerabilities that exist while doing business on the internet. Lawyers in virtually all practice areas have been seeing issues involving cyber risk arising with their clients more frequently. On a parallel course, a professional standard of care is developing that requires lawyers to have at least enough understanding of technological vulnerabilities to spot the issues. Consider the following hypothetical case as an example of a situation that lawyers are commonly encountering.

A Case Study in Standard of Care

A company operating convenience stores in Texas experiences a data breach involving a theft of its customers' credit card information from its computer network. The company learns of

---

http://oag.ca.gov/system/files/Richard%20Berger%20CPA%20Ad%20resubmit%207_22_15_0.pdf? (last visited Aug. 15, 2015).

[5] OTA Determines Over 90% of Data Breaches in 2014 Count Have Been Prevented, Online Trust Alliance, *at* https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented (last visited Aug. 15, 2015).

[6] *Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data*, Ponemon Institute, *at* https://www2.idexpertscorp.com/fifth-annual-ponemon-study-on-privacy-security-incidents-of-healthcare-data (last visited Aug. 15, 2015).

the breach from its credit card processor which requires that the company obtain a Digital Forensics and Incident Response (DFIR) investigation from a Qualified Security Assessor (QSA) to determine how the breach occurred as well as whether the convenience store complies with Payment Card Industry Data Security Standards (PCI DSS).

The company turns to its long-time business lawyer for advice on how to handle the situation. The lawyer, an excellent trusted-advisor who has served this company well for decades, tells the company what many lawyers would say, in a situation involving a potential crisis, that has remained relatively secret: "you never have to explain what you never said – if news of this has not gone public, just stay quiet about it and hope it passes." Unfortunately, the company's lawyer had never heard of Texas' Data Breach Notification Law[7] and certainly had no idea what DFIR, QSA, or PCI DSS mean.

The lawyer saw this as some "technology nonsense--not law," and took a back seat. The company, on its own, moved forward with obtaining the investigation, which cost the company thousands of dollars out-of-pocket, many man-hours from the company's IT team, and a measurable disruption in the company's business when its Point of Sale (POS) payment system had to be taken offline when it was found to be infected with malware and the company had no Security Incident Response Plan in place to respond to such an event. Predictably, the QSA's investigation found the company's computer network had been infected with malware for many months prior to its learning of the breach.

Unfortunately for the company, litigation ensued about a year later. During depositions after about a year of litigation, the issue of cyber insurance came up. In the next break, the CEO of the company asked its lawyer about cyber insurance and whether the company had this coverage. The lawyer, having never heard of cyber insurance, said "nope, I've looked at all of the documents you sent me and I have never heard of such a thing."

Following that break, the attorney taking the deposition began to dive deeper into the company's insurance policies and that is when things began to get even more intense. It turns out, the company had multiple policies that provided some level of coverage related to data breaches and, when combined, the coverage was substantial. The policies provided coverage for the QSA's investigation and for the incident response process in order to comply with the law of Texas, as well as those of other states. For negligence-based claims against the

---

[7] *Two Step Data Breach Risk Test for Texas Businesses*, Business Cyber Risk Law Blog, at http://shawnetuma.com/tag/texas-data-breach-law/ (last visited Aug. 15, 2015).

company, that arose from a data breach, the policies provided coverage for litigation expenses and defense of negligence-based claims.

There was one very important condition precedent to such coverage. Upon learning of the event of loss, the company had a duty to immediately notify its insurance carrier, and all claims had to be made and reported within one year of learning of the event of loss. If these conditions were not satisfied, there was no coverage. Period.

What Should a Reasonable Attorney Do?

A reasonable business attorney needs to do three things when it comes to cyber insurance.

First, a reasonable attorney must understand that in the current business climate, it is a virtual certainty that businesses will have a security incident that results in a data breach. It may be a sophisticated cyberattack caused by a crime ring; or, more likely, it will be something as simple as an employee taking information he is not entitled to have, or losing a mobile phone with access to the company's server and customer data. Regardless of the nature of the security incident, a reasonable attorney should assume his or her clients will experience a data breach and be prepared to advise them accordingly.

Second, when representing a business client in an ongoing relationship, a reasonable attorney needs to have at least enough knowledge of cyber insurance to raise this option with his or her clients, inquire as to whether they have considered the pros and cons, and offer some general advice on how such coverage can help protect their companies.

Third, when a client informs a reasonable attorney that it has had a security incident that could result in a data breach (as well as a litany of other cyber events), the reasonable attorney needs to ask the client about its insurance coverages, explain what cyber insurance is and how it can help in such situations, and request to review the policies to determine whether or not there is coverage available. Finally, the attorney should document that he or she followed all of these steps.

What is Cyber Insurance?

While most business professionals are just beginning to hear about it, cyber liability insurance is not a new product or a newly uncovered risk. It has been around for over 35 years and was first introduced in the 1980's. "Back then, technology companies bought errors and omissions (E&O) insurance, which over time, was extended to include things like a software product bringing down another company's network, unauthorized access to a client system,

destruction of data, or a virus impacting a customer."[8] Today, cyber coverage can mean different things to different people. To simplify some language, let us use the term "Cyber Liability" to encompass the components of this risk. This is to say that all companies that use a computer, receive, store, or transmit electronic data, or connect to the Internet are exposed to Cyber Liability. Cyber insurance is designed to cover Cyber Liability, among other things.

How Do You Help Your Clients Evaluate Cyber Insurance?

The most important action to take is to make sure that your clients understand the need for cyber insurance and that it is available. Beyond that, it is helpful if you have a good working relationship with insurance professionals who are experienced with cyber insurance and can help you advise your clients. It is usually best to introduce them to at least two options so that they can hear different perspectives and not feel as though you are pressuring them into buying something from a buddy.

How Will Experienced Insurance Professionals Help?

Experienced professionals can offer advice on solutions that can help protect your client from suffering a large financial or reputational loss due to cyber risk. Assuming that companies will face Cyber Liability risk and losses will happen, experienced risk management professionals can help with risk mitigation as well as risk financing (through insurance contracts).

They will do this by first helping clients identify the risks associated with their business operations. This requires taking a step back from the hazard risk, or the risks generally covered via insurance and looking at risk as a whole. They will look at it from a business, strategic and hazard perspective. From there, they will step back even further and help educate your clients on how to manage each of their risks in the following ways: prevention, mitigation, transfer, financing and assumption of risk, just as experienced legal counsel would do. For Cyber Liability, they will focus on risk mitigation and risk financing techniques. To assist in this process, there are some key questions that your clients should consider:

- How would a cyber-attack, data breach or data hijack impact their on-going operations?
- How much would their reputation suffer?
- Do they have a plan in place to respond to a breach and help mitigate loss, in the event of a breach?

---

[8] Laurie Floresca, *Cyber Insurance 101: The Basics of Cyber Coverage, at* http://www.wsandco.com/about-us/news-and-events/cyber-blog/cyber-basics (last visited Aug. 15, 2015).

Any answer other than a resounding "YES" means your client needs to spend some time analyzing the impact of Cyber Liability on their business with both you, as legal counsel, as well as a qualified insurance professional who understands how to assess a company's exposure to cyber liability.

What Kinds of Policies Offer Coverage for Cyber Liability?

The sheer number of data breaches that have been publicized and documented in the news has created multiple discussions on coverage. Perhaps the most frequently asked question is "is Cyber Liability covered under general commercial policies?" The short answer is "yes," usually there is limited coverage. There have been notable cases that have driven the need to standardize Cyber Liability insurance products as well as re-vamp current General Liability policy language. For example, a Commercial General Liability (CGL) policy may provide coverage for allegations of liability resulting from a data breach. This type of loss may trigger the insuring agreement of Coverage B: Personal and Advertising Injury Liability. However, the legal wrangling over these issues is still unresolved and the insurance industry has responded by taking steps to carve out "data-related liability" from the CGL insurance policies via a new exclusion. This has helped to eliminate ambiguous and vague policy language. But, has also created the need for companies to purchase additional policies to ensure they do not have gaps in coverage.

Companies that have Directors & Officers Insurance may find there is limited coverage affording protection against Cyber Liability. To the extent it exists, however, this coverage would provide coverage for the individual directors but not the company itself. The company would need to obtain additional coverage.

Commercial Property insurance may also provide limited coverage for Cyber Liability. The policy language can vary significantly across carriers, and many insurers exclude coverage for loss of electronic data (specifically defined in the policy) or provide sub-limits for those specific exposures. This coverage may allow for an insured to submit a claim and be reimbursed for the hardware, systems, recreation of files and business interruption; but, will not provide costs for regulatory fines, notification to third-parties, credit card monitoring, and other expenses associated with responding to a data breach.

Not all coverage is created equal and it is important for your clients to match their cyber insurance policy needs with their business operations and risk. Every business has its own unique vulnerabilities and there is no one-size-fits-all approach. This is where the advice and guidance of experienced insurance professionals, working with experienced legal counsel, can

really benefit the client. There are, however, several core elements for which a quality cyber insurance policy should provide coverage, including the following first-party costs:

- Legal and forensic services to determine whether a breach occurred and assist with regulatory compliance if a breach is verified.
- Notification of affected customers and employees, including costs such as letter preparation and mailing.
- Customer credit monitoring and identity protection services.
- Crisis management and public relations to educate the company's customers about the breach and protect its company's reputation.
- Business interruption expenses such as costs for additional staff, rented or leased equipment, use of third-party services, and additional labor arising from a covered claim.
- Cyber extortion reimbursement for perils including credible threats to introduce malicious code; pharm and phish customer systems; or corrupt, damage, or destroy their computer system.

Such a policy should provide coverage for the following third-party defense and liability costs:

- Judgments, civil awards, or settlements the company is legally obligated to pay after a data breach.
- Electronic media liability, including infringement of copyright, domain name, trade name, service mark, or slogan on an intranet or Internet site.
- Potential coverage for employee privacy liability as well as network security and privacy liability.

Finally, it is important to review the potential policy language for basic insurance coverage issues such as deductibles, sub-limits, total limits as well as specific exclusions. There are a few key items that may not be covered:

- Reputational harm.
- Loss of future revenue (for example, in the case of Target if sales were down due to customers staying away after data breach).
- Costs to improve internal technology systems.
- Lost value of the company's own intellectual property.

Not every lawyer needs to be an expert on cyber law, however, a basic familiarity with the issues is helpful. As your clients' trusted advisor, it is important for you to have enough

understanding of cyber risk to at least raise these issues with your clients and advise them on how they can seek additional protection, such as cyber insurance. In the right situation, that advice can be invaluable to your clients. This is just a cornerstone of practical lawyering in the 21st Century.

About the Authors

Shawn Tuma (@shawnetuma) is a business lawyer with a nationally recognized reputation in cybersecurity and data protection law. Business leaders regularly trust Shawn to help solve problems with cutting-edge issues involving cybersecurity, data privacy, computer fraud and intellectual property law. He is a Partner in the Cybersecurity & Data Protection Law Section at Scheef & Stone, LLP, a full-service commercial law firm in Texas that represents businesses of all sizes throughout the United States and, through its Mackrell International network, throughout the world.

Katti Smith is a 14-year veteran of the insurance industry and recently joined AIG, a world leader in Insurance as a Sr. Business Development Manager. She is a student of the industry and is passionate about educating her clients to ensure they are aware of emerging risks within the industry. She has obtained several industry specific designations, including her CPCU, RPLU and ARM and is a Licensed Risk Manager.