Best's Insurance Law Podcast

Minimizing Cyber-Data Breach - Episode # 113

Posted: Wed., Feb. 10, 2016

Hosted by: John Czuba, Managing Editor
Guest Attorney: Ted Schaer of Zarwin Baum DeVito Kaplan Schaer Toddy, P.C.
Qualified Member in *Best's Recommended Insurance Attorneys* since: 1993

ZARWIN • BAUM • DEVITO
KAPLAN • SCHAER • TODDY • P.C.
ATTORNEYS AT LAW

Announcer: Welcome to the Insurance Law Podcast, brought to you by *Best's Directory of Recommended Insurance Attorneys*.

John Czuba: Welcome to the Insurance Law Podcast, the broadcast about timely and important legal issues affecting the insurance industry. I'm John Czuba, Managing Editor of *Best's Directory of Recommended Insurance Attorneys*.

We're pleased to have with us today, attorney Ted Schaer from the law firm of Zarwin Baum DeVito Kaplan Schaer Toddy P.C. in Philadelphia, Pennsylvania. Ted Schaer practices law in Philadelphia and New Jersey, and is the Chairman of the firm's Cyber Liability, Privacy and Data Protection Department. Ted is also serves as the Firm's Chief Information and Security Officer. He routinely advises his clients on matters involving data security, cyber liability and insurance coverages as well as Best Practice compliance in the storage and maintenance of data. Ted has his CIPP\US certification.

Ted has practiced law for over 29 years and has tried over 50 jury and non-jury matters to verdicts. He is a Board certified trial attorney.

For the 3rd year in a row, Ted won the prestigious Magna Legal Services national mock trial contest, "CHOPPED," which helped raise money and awareness for the Children's Hospital of Philadelphia. In 2015 Ted was also appointed as a co-Dean of the CLM School of Cyber Claims. He will oversee the faculty and the Executive Council of claims professionals for implementing and instructing the school's cyber claims and coverage curriculum which is a three-year course resulting in a certification for successful completion.

Ted we're very pleased to have you with us again today.

Ted Schaer: John, thank you and thank A.M. Best for this opportunity.

John: Today's topic centers on the steps that a business can take to help prepare for and minimize the chances of a cyber data breach. Ted, can you start off by telling us what costs a business faces when we're talking about a cyber breach?

Ted: Sure. John, even before we get to that, the issues facing all businesses today – small, medium and big businesses – what can we do to protect our company from being a victim of cyber fraud, and the very significant monetary damages and reputational harm that will result when your data is breached.

We look at the very influential and important Verizon study of 2015 on data breach. What we know is that the crown jewels- what these criminals are after is information – personal identifiable information, personal health information and PCI, payment card information. Those are the crown jewels.

That study tells us that the average settlement is about $880,000. The average legal cost is well over $400,000. The average crisis services are about $500,000. What we know is that for the average record lost, it's about $200 per record. You do the math, and you realize a business loses 100,000 records, that's a lot of money.

John: Ted, can you tell us where the greatest threat today is for a breach? Is it an international hacker, a cybercriminal or something else?

Ted: Most people on the outside, who are looking at the problem of data breach and security, automatically assume that the problem is a hacker somewhere in Europe or in China trying to enter their network. While that may be true in some instances, our studies are telling us that the majority of attacks, 37 percent are coming from malicious attacks, 29 percent are coming from actual system glitches, and 35 percent is coming from human negligence.

That means lost computers. It's lost iPhones. It's lost iPads. It's employees who are not properly trained, and are falling for phishing scams and other scams that are allowing the bad guys to get into the networks.

John: We hear a lot about performing a risk assessment. Why is that important when considering cyber exposure?

Ted: Every business has to evaluate exactly what their network is and what they've got. When we talk about a cyber risk assessment, we're talking about evaluating where the weak link is before the bad guys find it. We're talking about businesses identifying internal and external vulnerabilities.

There are businesses that are trying to understand how to detect and how to respond to cyber threats. The things that businesses need to be considering when they're doing these cyber risk assessments are vulnerability assessments, penetration testing, physical security assessment, and of course, wireless security assessment.

What we see is in terms of vulnerability, we see technical exposure. We see companies that are practicing what we call "poor cyber hygiene." We see companies that are allowing access to corporate networks without special security. We see companies that are not tracking mobile devices, such as laptops and tablets, and a disdain for multi factor authentication for email and data access.

When a company performs a cyber risk assessment, they start evaluating and seeing their own inefficiencies and deficiencies which, are leading to these cyber breaches, and ultimately, leading to the type of financial harm that the 2015 Verizon report is telling us out there.

John: Is risk assessment industry specific?

Ted: It can be. Certainly, every industry has a specific risk, but there are risks that are germane to all businesses that we just talked about briefly. We look at things like the National Institute of Standards and Technology, NIST. These are standards which apply across the board and set standards for all businesses, like when logs and files should be backed up, retention periods for archived log files.

We look at standard based assessments to determine what laws, and regulations and standards apply to any given industry. As an example, if you're in retail or you're in the hospitality business, we look at the payment card industry data security standards, also known as PCIDDS. This applies to those businesses that are holding and securing credit card information.

Investment firms look to SEC safeguard rules, and of course, healthcare looks to HIPAA and things like that. Yes, every industry and every business has its own industry standards and regulations that we look to in order to form opinions regarding risk assessment, and how we're best going to protect ourselves against it.

John: What about the development of policies and procedures for cyber security?

Ted: That is certainly an important task for all businesses to consider. As we all know, it's not a question of if but when, in terms of a cyber attack, and securing of data, and personal information and PHI. It is important for a company to think about cyber policies before you have an incident.

As an example, creating a committee of the stakeholders whether that's the folks in the IT department, the C suite or risk management. These are the folks that need really to code, devise and drive policies for their company in order to limit, or minimize, the risk of cyber exposure.

Having policies on information privacy, on encryption on mobile devices, having policies on how to handle new vulnerabilities, and how they can be protected and how they can be detected. Of course, creating a rapid response team, and practicing for a breach in a tabletop exercise, is essential for any business and every business that stores data, and personal identifiable information, and PHI and PCI of its customers and its employees alike.

John: Ted, what types of insurance are in the marketplace, which conceivably could cover cyber breach?

Ted: Having insurance first is critically important to anybody that is holding data that is potentially available for breach. In today's insurance environment, certain types of damages arising from a cyber breach can be found in a GL policy. Sometimes they can be found in errors and omission.

A shareholder derivative suit is brought against folks in the board, DNO. Certainly crime, theft and plastic policies can offer protection, depending on the nature of the loss and depending on the wording on the policy.

Of course, cyber policies can as well. That, I think, is what folks have to really think about that today there are in fact standalone cyber policies that are out there. Each business needs to ensure that the coverage that is being offered and the limits that are being obtained meet each company's needs.

Unlike the policies that we just talked about, the cyber policies are manuscript policies. There are no ISO forms that deal with one specific cyber policy. It's very important when a business is out in the marketplace, and dealing with their insurance broker determining the type of cyber protection that they need, that they understand what their vulnerabilities are.

That they understand the type of information that they have, and that they understand the kind of risk that they need to protect and negotiate within the policy, and within the language of those policies, in order to adequately protect themselves from the risk that they have and the exposure that they're exposed to.

John: Ted, thanks very much for joining us again today.

Ted: Thank you so much.

John: That was Ted Schaer from the law firm of Zarwin Baum DeVito Kaplan Schaer Toddy P.C. in Philadelphia, Pennsylvania. Special thanks to our producer today, Brian Cohen. Thank you all for joining us for the Insurance Law Podcast. To subscribe to this audio program, visit Podcast.InsuranceAttorneySearch.com, or go to online directories, such as iTunes, or Google or Yahoo's podcast directory.

If you have any suggestions for a future topic regarding an insurance law case or issue, please email us at lawpodcast@ambest.com. I'm John Czuba, and now this message.

Transcription by CastingWords

To find out more about becoming a qualified member in *Best's Insurance Professionals & Claims Resource*, contact claimsresource@ambest.com or visit our Get Listed page to start the application process.

BEST'S RECOMMENDED INSURANCE ATTORNEYS AND ADJUSTERS