Best's Insurance Professionals and Claims Resource

Attorneys, Adjusters, Auditors, Expert Service Providers, Third Party Administrators, and Legal and Claims Officials

Best's Insurance Law Podcast

Attorney Discusses Impact of Cyber Liability on Businesses - Episode #104

Posted: Thu., Feb. 26, 2015

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

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, PC, in Philadelphia, Pennsylvania.

Ted is the Co-Chairman of the firm's Casualty and Defense Department, and is the Chairman of the firm's Cyber Liability, Privacy, and Data Breach response team. Ted is licensed to practice law in Philadelphia and New Jersey, and has been in practice since 1987.

He has tried over 50 jury trials to verdict, and has selected an additional 50 jury panels. Ted has represented insurance companies and their insureds in a variety of matters, including general, liquor, and professional liability matters. He is board certified, and a trial attorney.

Ted has also been certified by the International Association of Privacy Professionals. This certification is the preeminent credential in the US private sector for privacy, data protection, and cyber breach response. Ted also serves as Chief Information Security Officer for his firm, and he counsels companies and their insureds on cyber liability, and responding to a data breach. Ted, thanks so much for joining us today.

Ted Schaer: Absolutely. Good morning.

John: Today's topic is on the impact of cyber liability on businesses. Ted, when should a client seek counsel from cyber counsel?

Ted: In the environment that we live in today, it really is no longer a question of if a business will be a victim of cyber-attack. It really is when a business is going to be a victim. All businesses need to prepare for that event. Any business that stores data that has value, personal identifiable information, or financial data is going to be a target.

We know from our experiences over the last several years that criminals are relentless. More, probably than not, a network of any business holding information, has already been breached. It is important for a business to reach out to experienced cyber counsel who can insure that the right team is assembled before a data breach occurs, and access to the network occurs.

John: In what areas of cyber liability can affect a client business?

Ted: The effect of cyber liability is far-reaching in businesses today. A cyber-attack can interrupt a business and prevent it from doing business. Cyber-attacks can cause disruption of equipment and the network, which is essential to a business's operation.

Cyber-attacks can result in lost business records. A cyber-attack can also cause a business to face regulatory fines from state, and local agencies. Reputational damage when a business has been attacked and their information has been compromised, clients begin to wonder whether in fact they can trust that business with their information.

Damages from lawsuits, from customers, and other businesses who have been affected by a cyber-breach, and certainly the costs associated with the breach response itself, are all areas where that liability arising from a cyber-breach can cause damage and harm to a business.

John: Ted, what is the action plan when a breach has been identified?

Ted: Hopefully, a business, before a breach has occurred, has put into place a plan to deal with a response. Hopefully, before they've identified, recruited, and trained members of what we call a Breach Response Team. Those members include executive leaders, and senior management in the company, in the C-suite, and identifying a company spokesperson.

Identifying people within the organization or an outside vendor who handles the IT, so when that breach occurs we are able to identify what data has been hacked, and disable the malicious code and the malware, which infiltrated the network. We're hoping that legal counsel and compliance counsel is in place in a breach, that the lawyer acts as the quarterback to the response.

They help direct the investigation, and direct the members of the team, and determine what agencies need to be notified. We need to have a crisis communication, or a public relations expert on hand and ready to deal with the fallout from the breach to the public, and to employees themselves.

Certainly, identifying a call center and a notification center, and setting up ID protection, making sure that law enforcement is identified at the right time, and placing cyber insurance claims people on notice, if in fact there is cyber liability, to put the claim into process.

When a breach has occurred, certainly the first thing that has to happen is to advise and activate that breach response team. Once that occurs, there has to be an identification of what kind of a breach occurred, and to stop the data loss while also preserving the forensic evidence.

ID-ing the compromised records is incredibly important to understand the regulatory responsibilities that a business faces. Activating a call center to begin the notification process to those customers, and those people whose records have been, in fact, compromised.

Notifying those individuals whose ID has been stolen, and those are responsibilities that are set forth in both state and federal laws. Making sure that an adequate protection mechanism has been put into place to protect those customers once that breach has occurred.

Communicating to all stakeholders, and shareholders, regulators, business partners, payment and credit card companies, and law enforcement, to advise them that a breach happened, and to ensure that they're doing everything that they need to do to mitigate that loss.

Then, of course, the final thing is to fix the issue that caused a breach. These are all basic skeletal outline of what has to occur in an effective breach response in order to mitigate damages and to not allow them to take a very bad situation, and make it even worse.

John: Ted, thanks so much for joining us today.

Ted: Good day.

John: That was Ted Schaer from the law firm of Zarwin, Baum, DeVito, Kaplan, Schaer, Toddy, PC, in Philadelphia, Pennsylvania. Special thanks to our producer Bryan Cullen. Thank you all for joining us for the Insurance Law Podcast. To subscribe to this audio program visit Podcast.InsuranceAttorneySearch.com, or go to an online directory, 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. Thanks for joining us. Now, this message.

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.