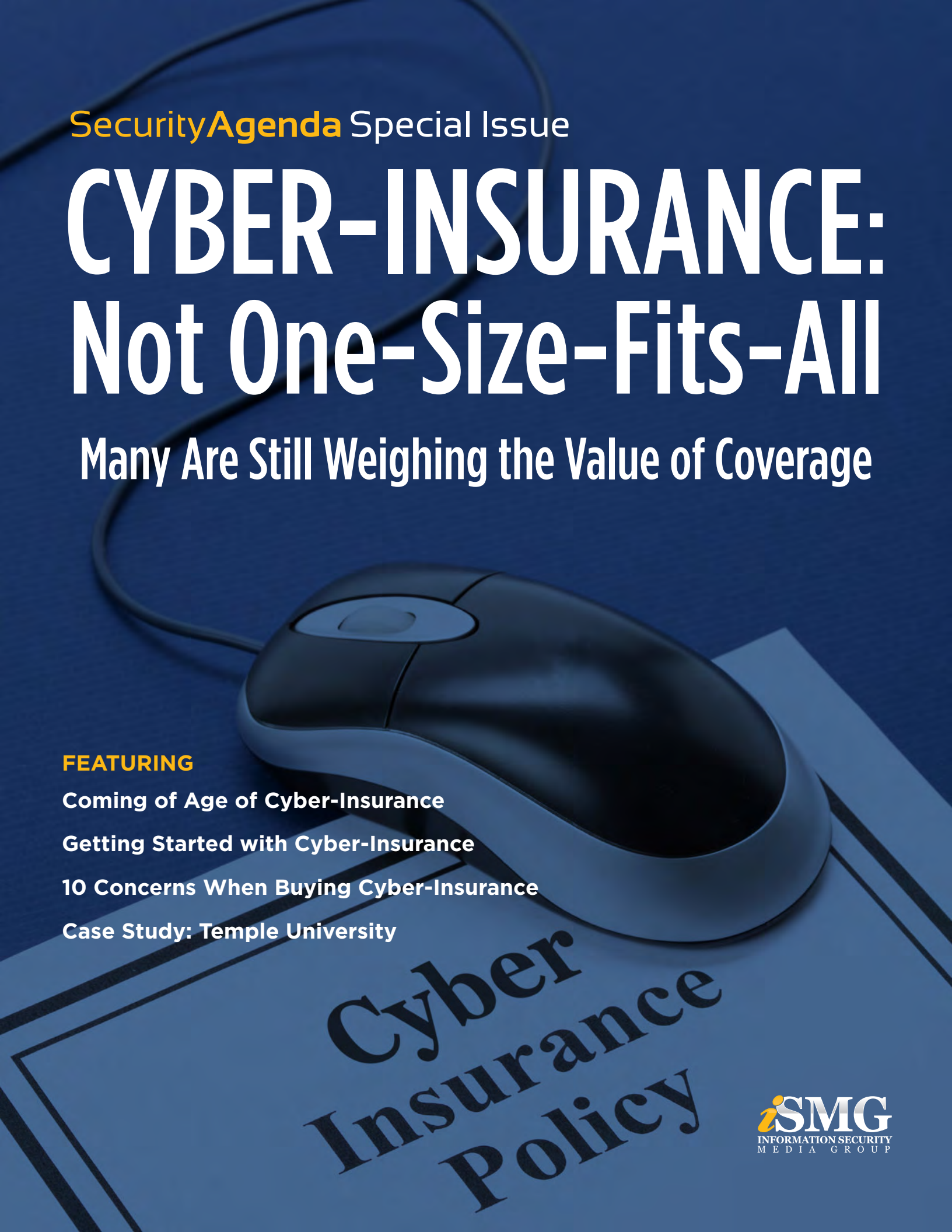
SecurityAgenda Special Issue

CYBER-INSURANCE: Not One-Size-Fits-All

Many Are Still Weighing the Value of Coverage



FEATURING

Coming of Age of Cyber-Insurance

Getting Started with Cyber-Insurance

10 Concerns When Buying Cyber-Insurance

Case Study: Temple University

ISMG
INFORMATION SECURITY
MEDIA GROUP

From the Editor

Cyber-Insurance: Helping Organizations Weigh Value of Coverage

Eric Chabrow
Executive Editor,
GovInfoSecurity &
InfoRiskToday

The not-too-old saw goes something like this: There are two types of enterprises: those that have been breached, and those that don't know it yet.

The likelihood is high that even those that don't know it yet will likely learn about their victimization by a cyber-attack soon enough. That's why most organizations can't – or shouldn't – manage risk these days without cyber-insurance. For most, they'd be foolish not to do so, considering that one study puts the average cost of a breach at $5.5 million.

Deciding what type of policy to buy and from whom to buy it isn't easy. The cyber-insurance marketplace is relatively nascent, at least when compared with other types of property and casualty insurance in the United States. There are about 40 insurers offering cyber-insurance vs. 5,000 for all other types of liability insurance.

The aim of this report is to help organizations weigh the value of their cyber-insurance coverage. In the following pages, we present articles on:

Cyber-Insurance: Not One-Size-Fits-All, explaining how cyber-insurance policies vary widely, but often cover notification expenses, credit-monitoring services, and, in many cases, legal defense costs and even government penalties. Basically, insurers offer two types of policies: first party covers direct expenses and third party covers payments made to others.

Coming of Age of Cyber-Insurance, detailing why cyber-insurance is joining a long list of other liability policies in an enterprise's insurance portfolio.

Getting Started with Cyber-Insurance, emphasizing a 3-step approach to initiate the process of acquiring cyber-insurance.

10 Concerns When Buying Cyber-Insurance, providing a check list of action items organizations should review when buying new or reviewing existing cyber-insurance policies.

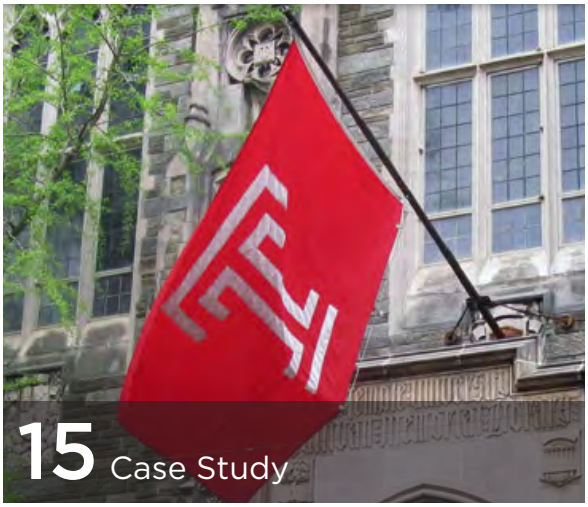
Case Study: Cyber-Insurance, exploring how Temple University went about deciding and buying cyber-insurance.

As we expand our cyber-insurance coverage, please help guide us by letting us know the type of articles and interviews we should pursue. Just e-mail your ideas.

Eric Chabrow
Executive Editor
Information Security Media Group
echabrow@ismgcorp.com

Cyber-Insurance: Not One-Size-Fits-All

5 Cyber-Insurance: Not One-Size-Fits-All

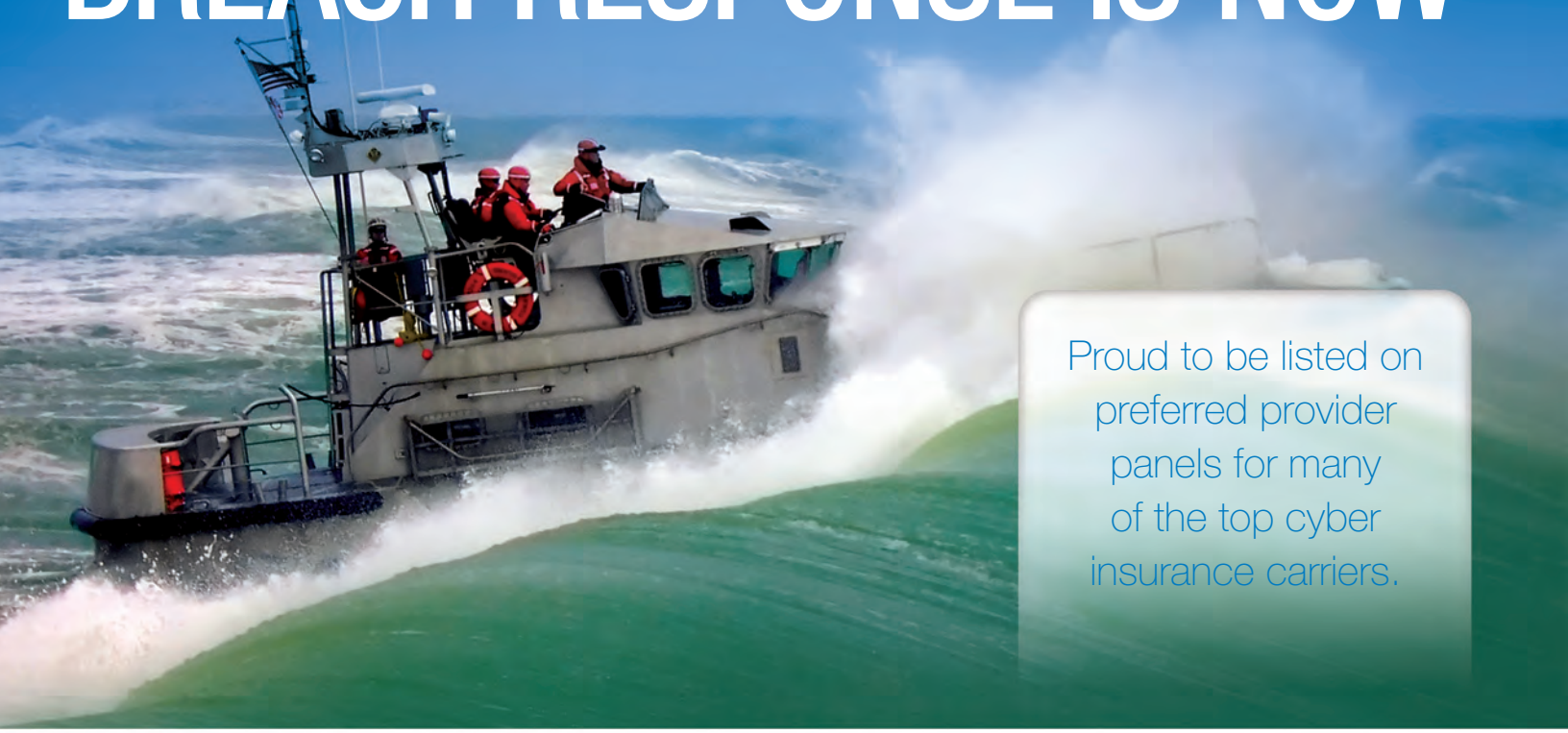


15 Case Study

Experian®

DATA BREACH RESOLUTION

THE TIME FOR ACCELERATED BREACH RESPONSE IS NOW



Proud to be listed on preferred provider panels for many of the top cyber insurance carriers.

Be more than ready. Be Experian® ready.

The risks are getting bigger, the regulations stricter, making data breach preparedness more important than ever.

Experian's fast, field-tested breach solutions help you:

- Be ready when a breach strikes
- Preserve customer loyalty and stakeholder confidence
- Reduce the likelihood of devastating penalties and fines

Contact Experian's accelerated breach response team at **1 866 751 1323** or **databreachinfo@experian.com** for a consultation.

Download the free Data Breach Response Guide at **Experian.com/DataBreachGuide** for comprehensive checklists, notification tactics and more.

Stay up to speed on breach response.

» Visit us online: **Experian.com/DataBreach**

» Follow us on Twitter: **@Experian_DBR**

» Read our blog: **Experian.com/DBBlog**

» Download our free mobile app for iPhone or Android

Cyber-Insurance: Not One-Size-Fits-All

Many Are Still Weighing the Value of Coverage

By Eric Chabrow

Despite headline-grabbing data breaches that have proven costly to organizations in many sectors, the purchase of cyber-insurance to cover potential costs remains relatively rare.

Cyber-insurance policies vary widely, but they often cover notification expenses, credit-monitoring services, and, in many cases, legal defense costs and even government penalties.

"Cyber-insurance is viewed as much more of a discretionary purchase, and risk managers really have to be educated on the need to purchase the coverage and what the coverage actually provides," says David Bradford, who published a 2012 survey that addresses cyber-insurance for RIMS, the risk information management society.

> **"Risk managers really have to be educated on the need to purchase the coverage and what the coverage actually provides."**
>
> - DAVID BRADFORD

"So far, that's been a little bit of a difficult sell for brokers," Bradford says. "Partially it's because it's a new product with brokers as well. A lot of them just don't really understand the products that well themselves. They don't do an effective job of indicating the need to the buyers."

Misperceptions

A 2012 survey of more than 100 global Forbes 2000 corporations by Carnegie Mellon CyLab shows that many board members and executives incorrectly

believe that other types of corporate liability insurance cover losses due to data breaches, says lab official Jody Westby.

"That's pretty stunning because most corporations, especially large global corporations, should understand that cyber-risks generally are not within property and general corporate liability policies," Westby says.

It's not just executives and board members who have yet to see a need for cyber-insurance. Corporate risk managers in many organizations, as well as a large number of the insurance brokers that corporations rely on to tailor coverage to meet specific exposures, don't fully appreciate what cyber-insurance offers.

No One-Size-Fits-All

Bradford estimates that 40 insurers offer cyberliability coverage. By comparison, about 5,000 companies provide property and casualty insurance in the United States.

Because the cyber-insurance industry continues to mature, its offerings aren't as consistent from provider to provider as they are with other types of insurance. "There are so many material differences between the coverages available that there is no real one-size-fits-all approach," says Richard Bortnick, an attorney at the law firm Cozen O'Connor.

What's covered by most cyberpolicies? Generally, they fall into two areas: first-party coverage, which covers direct expenses, and third-party coverage, which covers payments made to others.

Examples of first-party coverage include notification expenses to alert stakeholders of a breach and provide them, when necessary, with credit-monitoring services, which insurer Chubb estimates could cost up to $30 per customer. Other first-party expenses include repairing reputation harmed by a breach, including public relations costs; restoring systems and data; repaying funds stolen through fraud or extortion; and covering revenue losses associated with computer system disruptions.

Third-party coverage encompasses court-imposed damages, regulatory penalties and defense costs associated with lawsuits alleging the disclosure of customers' personally identifiable information or harm to business partners' systems.

> **"Corporate risk managers in many organizations don't fully appreciate what cyber-insurance offers."**

An organization's decision on what type of policy to buy and what it should cover depends, in part, on the type of information that could be exposed.

"To the extent that an entity has a large number of personally identifiable information records, then there's a much bigger chance of exposure," says Kevin Kalinich, global network and cyber-risk practice leader for Aon Risk Solutions, an insurance brokerage. In general, businesses with such exposures include retailers, hospitality providers, healthcare providers, health insurers, financial institutions, payments processors and educational institutions, including colleges and universities.

> **"There are so many material differences between the coverages available that there is no real one-size-fits-all approach."**
>
> - RICHARD BORTNICK, COZEN O'CONNOR

Assessing Existing Coverage

Temple University sought cyber-insurance after other schools suffered breaches and its director of risk management and insurance, Lisa Zimmaro, realized that its general liability policies didn't protect it from losses related to its computers and information systems [see Temple University Invests to Protect Assets, p. 11].

"There are a lot of exclusions in general-liability policies that made us think that had we had a breach, our general liability carrier would deny coverage," Zimmaro says.

But businesses that don't retain a lot of personally identifiable or sensitive information on their computers would likely choose far more limited cyber-insurance coverage, if any at all.

Ace Hardware, a cooperative of 4,500 stores owned by individual retailers, bought a limited policy because the parent organization stopped processing credit card information several years ago, says William Montanez, director of risk management. Its cyber-insurance is limited to coverage of legacy exposures.

The Cost of Breaches

Still, for many organizations, data breaches and exposures can prove costly.

A hack of South Carolina's tax system in 2012 is expected to cost the state at least $20 million, mostly for the costs to notify 4 million taxpayers whose personally identifiable information was exposed and provide them with free credit-monitoring services, according to the news website GreenvilleOnline. The federal and state governments generally self-insure, but smaller local governments often rely on insurance.

Although most data breaches aren't as costly as the one South Carolina experienced, they can make a dent in an enterprise's coffers. The average breach costs an organization $5.5 million, according to the 2011 Cost of Data Breach Study conducted by the Ponemon Institute. The typical breach exposes more than 28,000 records at a cost of $194 a record that includes notification, call center, forensics and other direct expenses.

Those types of losses may eventually prompt more organizations to seek cyber-insurance. But John Wheeler, a research director at IT consultancy Gartner, cautions that cyber-insurance isn't a stopgap measure to compensate for weaknesses in an IT security program. ■

To read the entire story, please go to:
http://www.inforisktoday.com/cyber-insurance-one-size-fits-all-a-5395

Coming of Age of Cyber-Insurance

Cyber Benefits from Shift to Enterprise Risk Management

By Eric Chabrow

Flip through the recent, 150-page RIMS Benchmark Survey and you'll notice lots of figures on payouts for auto, aviation, fiduciary, marine, malpractice, worker's compensation policies and so on, but not much on cyber.

"Cyber exposure is increasingly a part of the concerns of the risk managers, but that is actually a relatively recent development," says David Bradford, the benchmark survey's editor. "Until just a few years ago, cyber exposure was conceived pretty much in the domain of the IT department, and risk managers didn't have a whole lot to do with it. In the past few years that has changed, but only about a third of large companies buy cyber-insurance policies."

Fifty-six percent of survey respondents said their organizations had not yet purchased cyber-insurance, while 38 percent said they had a policy and 6 percent didn't know.

The survey results are indicative of what's occurring in the marketplace but don't purport to show exact amounts being paid out by cyber-insurers. But Bradford predicts more organizations will purchase cyber-insurance in the years to come - and risk managers will become more involved in buying the policies.

Taking a Broader View of Risk

Organizations have been assessing risks in silos rather than enterprisewide. Risk managers have viewed risk narrowly; for example, by assessing liabilities resulting from fiduciary responsibilities separately from, say, workmen's compensation. Not that they aren't and won't continue to be assessed independently, but over the past decade or so, enterprise risk management has been gaining momentum. And because information technology deals with nearly every aspect of an organization's operation, assessing cyber-risks fits neatly with the trend toward enterprise risk management.

"As far as data security goes, increasingly companies are looking at it as an enterprisewide problem and not just something that sits on the servers in the IT department," Bradford says. "And, it's especially the case now that more and more companies have employees with mobile devices that are connected to the system that could be lost or stolen. More and more companies are creating committees that span the organization to address data security issues, and increasingly that includes the risk management department."

"More and more companies are creating committees that span the organization to address data security issues, and increasingly that includes the risk management department."

- DAVID BRADFORD

The movement toward assessing cyber-risks as part of enterprise risk management is just one more piece of evidence that supports the contention that information security is becoming too strategic for organizations to be ignored by anyone - including risk managers. ■

http://www.inforisktoday.com/blogs/coming-age-cyber-insurance-p-1325

Getting Started with Cyber-Insurance

Assessing the Type of Cyber Coverage to Buy

By Eric Chabrow

How should organizations considering cyber-insurance start the process? Cyber-liability lawyer Richard Bortnick offers three steps in determining the type of cyber-liability coverage they should seek.

"Policy holders are not necessarily being given the best advice or they don't understand the scope of the coverage that they have," he says.

For organizations mulling the purchase of cyber-insurance, Bortnick offers the following three tips:

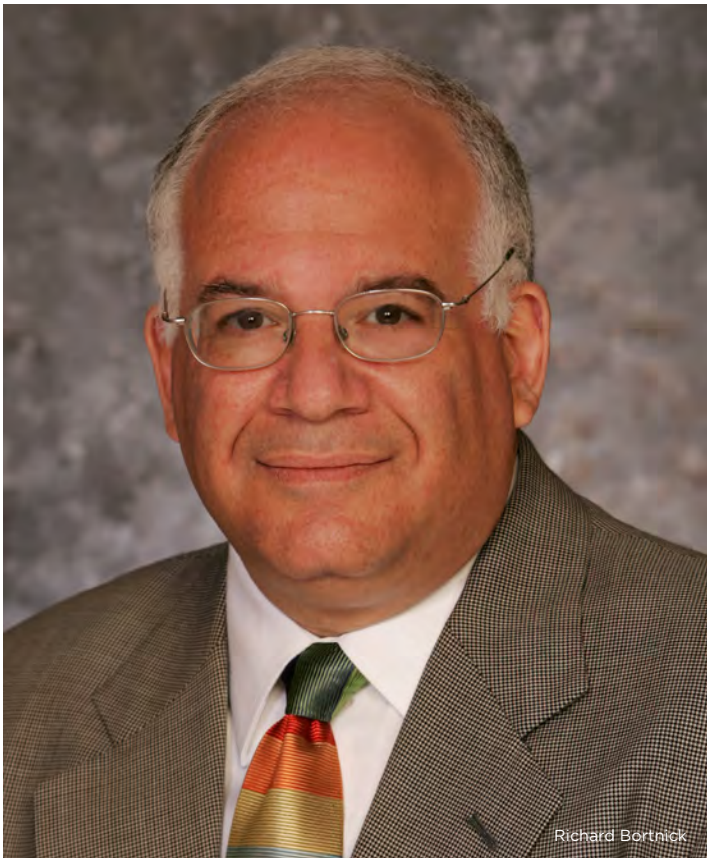
- **Conduct an initial risk assessment:** The assessment should be top-to-bottom and consist of the internal risks to the organization as well as the potential exposure of sensitive information in order to determine which type of cyber-liability insurance coverage they should seek, Bortnick says.
- **Speak with a lawyer:** Seek advice from a lawyer, Bortnick says. They should be willing to provide free advice since the information being sought shouldn't take that long for a lawyer to provide.
- **Create a cyber-response plan:** This process involves developing a team consisting of members from various departments in the organization, such as general counsel, IT, human resources and management. "You need everybody to get in a room, discuss what the corporate assets are that need to be protected, what the personal information is, whether it's employees or customers or clients, and come up with some kind of plan to send people off to do their respective jobs," he says.

What follows is an excerpt from an interview with Bortnick, where he explains why most organizations are not properly insured against cyber-attacks and IT failures.

Cyber-Insurance Usage

ISMG: Are most organizations properly insured against the impact of cyber-attacks and IT failure?

BORTNICK: The vast majority at this point are not. Most companies still to this day do not appreciate the risks and exposures that they face and are not aware of exorbitant costs that could arise from a cyber-breach, both with respect to business interruption loss as well as third-party exposures, should financial, healthcare or other information of customers' clients be stolen. There are a lot of



Richard Bortnick

"Most companies still to this day do not appreciate the risks and exposures that they face and are not aware of exorbitant costs that could arise from a cyber-breach."

- RICHARD BORTNICK, COZEN O'CONNOR

"It's like the shoemaker whose son walks around barefooted. It can't happen to me. I don't worry about myself. I'm worried about everybody else."

- RICHARD BORTNICK, COZEN O'CONNOR

different verticals that companies need to be concerned about: first-party, crisis-management and third-party liability.

ISMG: There's a lot of news about cyber-intrusions and then companies being hacked and personally identifiable information being exposed. Despite this, why do you suspect that companies aren't aware?

BORTNICK: It's like the shoemaker whose son walks around barefooted. It can't happen to me. I don't worry about myself. I'm worried about everybody else. You read about cyber-breaches and virtually all that you know about are big Fortune 50, Fortune 100 companies and government contractors - folks that the typical company or the typical person who owns the company can't relate to. They presume, "Why would someone hack me? Who would want anything that I have?" I would say to them, "If you had an opportunity to rob a bank in downtown Philadelphia where I'm located or you could go into a suburb on a street corner that's a neighborhood, where would you go?" The low-hanging fruit is the easy street-corner bank, and the low-hanging fruit in this space is smaller, mid-sized companies that either don't appreciate the risks or don't think it can happen to them. These companies are not out there actively putting into place the cybersecurity protections that they might need, or thinking about having to buy insurance because they're investing their limited corporate assets in other things to grow the business, and not thinking about protecting the business.

ISMG: Is there a perception, or misperception, among many organizations that they have other types of liability policies that might protect them from some of the damage that can be caused by a cyber-attack?

BORTNICK: Let me answer that this way: yes and no. Companies don't think about it. They just don't. It's not on their radars until it's on the radars. As to those companies that have thought about it, they will most likely have asked their brokers. Sadly - even as of today - brokers don't understand the product. I had a broker say to me such and such a client did not need cyber-insurance because they have a different type of insurance. Well I looked at their coverage and came to realize, very quickly, they didn't have the coverage the broker said or thought they did.

Policy holders are not necessarily being given the best advice or they don't understand the scope of the coverage that they have. Some policies do provide limited coverage. For example, there was a recent decision that came out from an appeals court that found a crime policy covered a cyber-event. Up to now, nobody was looking at crime policies so there's one other avenue that a company could look to if you're a service provider. You might look to your professional liability policy for third party. That still does not address the first-party business interruption. It certainly doesn't address the crisis management aspects, which up to now has been the leading expense in this area. Lawyers are second and liability with regard to third-party lawsuits is way down the list of expenses. Folks who think about it think they're covered, but, depending on the type of event that we're talking about, they might not be. They probably aren't. ■

A frequent lecturer and blogger on cyber-liability and insurance, Bortnick is a member resident of the law firm Cozen O'Connor's Philadelphia office. He is the Pennsylvania chair for the Council on Litigation Management. Bortnick co-chairs the Computer and Technology subcommittee of the American Bar Association's Insurance Coverage Litigation Committee.

---

http://www.inforisktoday.com/interviews/cyber-insurance-getting-started-i-1660

The Role of Cyber-Insurance in Breach Response

Experian's Michael Bruemmer, Attorney Ronald Raether on Strategy

By Tom Field

It could be a distributed-denial-of-service attack against your organization, a breach of one of your third-party vendors, or perhaps one of your trusted employees has lost or had stolen a mobile device containing personally identifiable information.

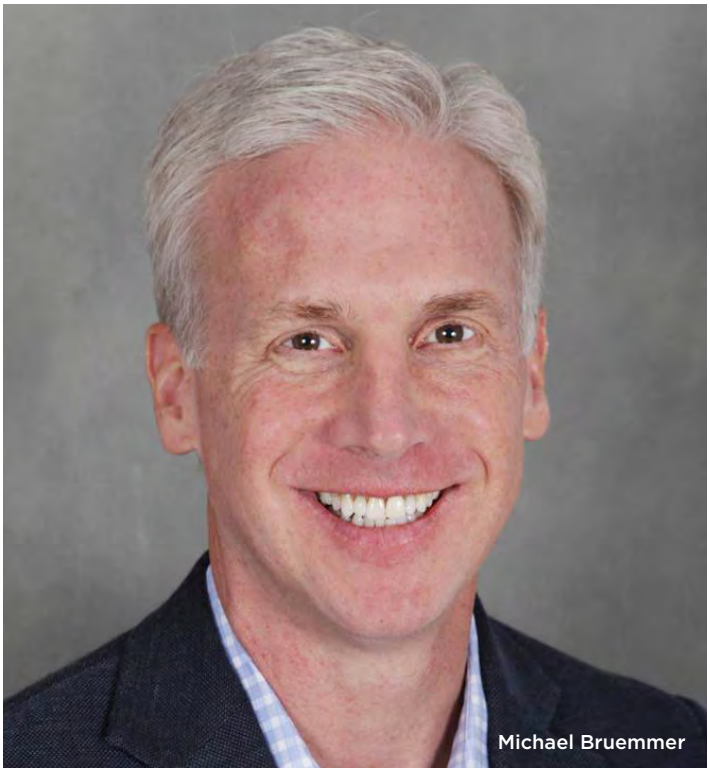
Whatever the scenario, data breaches are increasingly common for organizations in all industries.

And while technology solutions for breach detection are growing more sophisticated, the strategic elements of breach response are not keeping pace, experts say.

Too often, breach response plans are left untested – until there is an incident. Often the strategies are not even communicated to all the stakeholders who need to be a part of the plan. That, or the plans fail to account for critical third-party vendors and their roles, including the cyber-insurance provider.

In this excerpt of an exclusive video interview, two prominent breach response experts discuss:

- Essential elements of a breach response plan;
- The emerging role of the cyber insurer.



Michael Bruemmer

Michael Bruemmer is Vice President with the Experian Data Breach Resolution group. A veteran with more than 25 years in the industry, Bruemmer brings a wealth of knowledge related to sales and operations. Most recently, Bruemmer served as the Business Development Director of Consumer Products at ID Analytics where he was responsible for the development and execution of all selling strategies.

"The one thing that cyber-insurers now have is a stake at the table."

– MICHAEL BRUEMMER

Ronald Raether is partner at Faruki Ireland & Cox in Dayton, Ohio. His experience with technology-related issues spans an array of legal areas, including patent; antitrust; licensing and contracts; employment; trademark; domain name disputes; and federal and state privacy statutes.

> **"Have a plan, test the plan, and follow the plan."**
>
> – RONALD RAETHER

Breach Response: What's Missing?

TOM FIELD: What do you find is typically missing in a breach response plan?

MICHAEL BRUEMMER: I actually think the biggest thing is third-parties. People don't consider the implications down the line for those people that they're outsourcing data to, even the subcontractors - especially now with the new final Omnibus Rule for healthcare.

RONALD RAETHER: I would say: Have a plan, test the plan, and follow the plan. And I think in doing that, companies will be better prepared. Unfortunately, somewhere along the line with respect to all three, companies have failed to do that. They either don't have a plan, they haven't tested it, or more importantly they don't follow it when a breach occurs.

Communication with Stakeholders

FIELD: What do you find is most commonly not communicated among the stakeholders about how they should respond to an incident?

BRUEMMER: In good incident response plans, people are saying, "Hey, regardless of what type of incidents, we need to plan for every eventuality." Typically, they don't talk about the explicit coverages of cyber-insurance because it's not necessarily relevant to every stakeholder. Finally, I would say the budget aspect. That's usually - if it's done correctly - done beforehand so that they're prepared. When it comes to the actual breach, it's all about execution.

RAETHER: I think that Mike is right. It's having the right people participating in the response, and having those people have some familiarity or knowledge about how they ought to react depending upon their individual roles. The CFO obviously has a role at the table, but likewise so does whoever is responsible for responding to the media. The chief security officer, the general counsel - all of them play a role, and they have to understand what their role is in order to effectively roll out an incident response plan.

Role of Cyber-Insurance

FIELD: Ron, one of the things that you've said in our conversations is that it's difficult to manage what could be competing interests in the wake of a breach. What do you mean by that?

RAETHER: One of the trends that we've seen recently is that, as outside vendors, we now have multiple masters. When the events first happened, we were normally dealing with just the company that owned or managed the consumer data, so we had one master at that point. Doing things like figuring out who needed to be notified; what needed to be included in the message; should we reach out to people that legally we're not required to notify, but should we do that anyway because it's the appropriate thing to manage the good will of the company - those types of questions are much easier to answer when you have a single master.

What's happened, especially in the HIPAA area and somewhat in finance in dealing with GLBA, is that you have contractors and subcontractors and sub-subcontractors.

We have that group of masters, and then we have cyber-insurance as another burgeoning participant in these breach responses. You didn't see a lot of cyber-insurance in '05, '06 and '07. You're seeing it a lot more today, and so you have yet another master that you're working with to try to put together the right and appropriate response.

BRUEMMER: The one thing that cyber-insurers now have is a stake at the table, in that they're the economic decision-maker. Whether you participate on a vendor panel with the cyber-insurer or you have an exclusive arrangement where the cyber-insurer controls every aspect and doesn't just allow you to pick from that panel, they're the ones that are saying, "Yes, you can notify. Here's how you're going to do it, and when you're going to do it, and this is the cost that we are going to allow you as part of the actual package." They have a very important stake in the process.

Key Elements of Breach Response

FIELD: What are the most important points to have in a breach response plan now?

RAETHER: It needs to be structured towards the facts and circumstances. I think too often there's a perception that it's a check-the-box type of response when you're dealing with the data breach, when in reality there's an art to being

> "It's the human interaction and the ability to make simple errors that have caused most of the breaches that we've been involved in the last few years."
>
> – MICHAEL BRUEMMER

able to understand what's involved in the incident; preparing the appropriate forensics study to determine who needs to be notified of precisely what happened; building all the facts that you're going to not only communicate to the consumers, but also the regulators when you have to go and speak with them; and then building not just the notice, but also the remedial measures that you're going to offer to the consumers.

BRUEMMER: I would add to that: Make sure with your incident response plan you actually practice it at least once a year. Within that plan, not only do you need clear processes and procedures, but the decision-making authority for the single person that's leading that response plan. They're speaking for the organization to the outside vendors, so have that single point of contact and that decision-making authority very clear to everybody participating.

Key Technologies

FIELD: Mike, in your experience, what technologies are commonly overlooked when organizations are looking to prepare a breach response plan or to employ it?

BRUEMMER: The technology of actual human interaction is the number-one issue because that's still the largest causal factor of any breach - employee negligence. There are plenty of technologies that are out there, but it's the human interaction and the ability to make simple errors that have caused most of the breaches that we've been involved in the last few years.

RAETHER: I can split the issue into two. One is breach avoidance, and the other is after the breach occurs. Mike has talked about breach avoidance, and there are a number of well-qualified people that are knowledgeable about what can be done and what can't be done, but I certainly agree that humans have been and will continue to be the weakest link in data security.

On the post-breach side, it's important that, depending on the type of the breach, the company goes in quickly and preserves all of the audit data. Systems create logs that tell who has been where and what has been accessed, and oftentimes those logs are overwritten in a short period of time - 24 hours, 12 hours, two days. Once it's gone, you can no longer recover or access that, and it becomes a critical component in being able to answer those questions that I talked about earlier: Who was affected? How were they affected?

Then, everything builds around the answers to those questions. If you've lost that data, if you're unable to do a true forensics analysis, it really hampers what we can do in our roles as vendors and, oftentimes, the consequences and overstatement of the exposure of the company.

Breach Response Trends

FIELD: What do you foresee as being the significant breach response trends of the year?

RAETHER: We've talked about the two things that I see. One is the collaborative aspect of data-breach response. For me personally, that was the discussion about masters and having to deal with multiple masters. Related to that is the cyber-insurance thing. While they're a master, I think the involvement of cyber-insurance and the issues that Mike talked about with respect to financing and response, all of those variations will come into play and our role will be to help navigate the company in making decisions on how far to go in terms of what's financed by the insurer, whether there's a little bit more that ought to be done and finding that funding within the company. Above and beyond the cyber-insurance, make sure that the good will of the company is maintained throughout the response of the breach.

BRUEMMER: If this year we come to the end of the year and read the headline that we had an uptick from previous years on the number of people that actually had an incident response plan and tested it regularly, like a 15- or 20-point increase year on year, I think that would make both Ron and I very happy.

To see the complete video interview on breach response, please view:
http://www.databreachtoday.com/breach-response-whats-missing-a-5590

10 Concerns When Buying Cyber-Insurance

Breaches Propel Organizations to Mull Insurance Protection

By Eric Chabrow

Interest in cyber-insurance rises with every report of a high-profile computer breach.

In 2011, 42 percent of one major broker's clients had cyber-insurance, up from 15 percent in 2008.

It's not only high-profile breaches that have peaked interest in cyber-insurance, but regulatory pressures, says John Wheeler, a research director at IT adviser Gartner. In the United States, the Securities and Exchange Commission requires publicly traded companies to disclose their cyber-risks as well as any cyber-insurance coverage they have. Also, Wheeler says, insurance brokers and providers have upped their marketing efforts.

Among the advantages of cyber-insurance: Protecting against a major cyber-risk, but one that can be specified. Some enterprises in industries such as financial services use cyber-insurance to meet regulatory requirements. Cyber-insurance could be beneficial to protect against easily valued losses such as regulatory fines and breach notification.

But, Wheeler cautions, organizations must measure those benefits against some of cyber-insurance's drawbacks. Cyber-insurance isn't a stopgap measure to compensate for weaknesses in an IT security program. Blank coverage for a broad array of low-limit loss events doesn't make sense. And, he says, don't buy insurance because of fear spawned by highly publicized cyber-attacks.

Unlike other types of liability insurance, there hasn't been enough history in claims and payouts for underwriters to know what to charge, several experts in the field say. At a recent Seton Hall University symposium on cyber-insurance, one presenter - from an insurer - said a dearth of experienced cyber-insurance underwriters exists. The lack of history and underwriters, several experts say, make it hard for insurers to know exactly how much they should charge for coverage.

"Cyber-insurance remains a gamble to insurance companies," says Paul Proctor, a Gartner vice president and distinguished analyst, comparing the risk insurers face to that of Lloyds of London, the famous British reinsurer that insured the legs of a celebrity dancer. If insurers bet wrong on cyber-insurance, they may not have the financial wherewithal to pay claims.

Gartner estimates cyber-insurance premiums range from $10,000 to $35,000 for $1 million in coverage.

What kind of coverage do the two dozen or so carriers offer? Various flavors of policies cover network intrusion; breach notification; loss of income and business interruption; regulatory civil action; and cyber-extortion and terrorism.

"Cyber-insurance isn't a stopgap measure to compensate for weaknesses in an IT security program."

At a recent security summit, Proctor outlined 10 considerations organizations should address when buying cyber-insurance:

1. **Buying into the sales pitch:** Most articles written about cyber-insurance are favorable. They should be taken with a grain of salt because most were sponsored by "somebody in the supply chain for cyber-insurance," Proctor says.

2. **Broker experience:** "There's already enough risk in this field," Proctor says. "Make sure you have someone on your team who has experience with actually working with clients who filed claims, not somebody reading the back of the policy to see what's in it."

3. **Policy complexity**: Lots of exclusions exist in cyber-insurance. Develop scenarios of cyber-losses to determine if an insurer will pay claims.

4. **Policy qualifications:** Claim processers often don't understand cybersecurity, such as advanced firewalls with malware protection. Are you covered if those protections were turned off? Ignorance here isn't bliss because that could lead to a denial of claims for items the insured might believe are covered.

5. **Pre-insurance survey**: Be careful and specific in filling out the forms that define the coverage you seek. Insurers could deny a claim if the insured says in the pre-insurance survey it employs an 8-character, alphanumeric password when a breached account password was "chocolate."

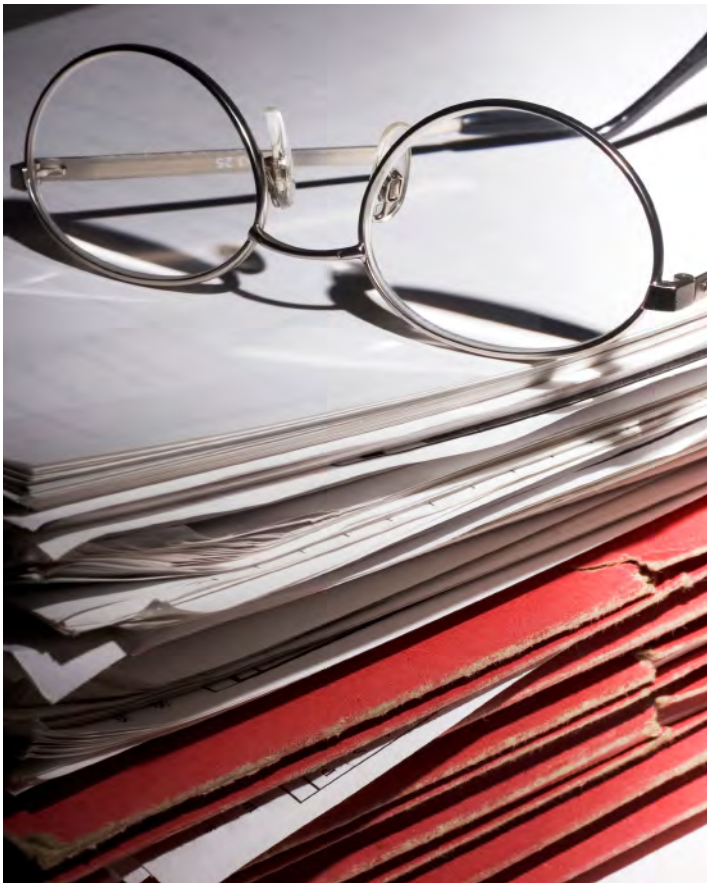
6. **Filing claims:** Cyber-insurance is a fairly nascent industry, with little known historically on how insurers pay claims. Indeed, insurers are just getting their sea legs, and providing cyber coverage remains a big risk for many of them. "If it's a gamble for them, it's a gamble for you," Proctor says.

7. **Selecting coverage**: There are many different types of coverage organizations can buy. "Think this through with your insurance team to make sure you get appropriate coverage, and which ones pay," he says.

8. **Understanding exclusions**: If an employee loads a program with malware on a computer, is that covered?

9. **The cloud**: Don't expect much protection for data in the cloud. Insurers cannot afford to payoff the risk for data stored in the cloud; it's not a sustainable business for them.

10. **Payment of claims**: Gartner says it has inconsistent information on whether insurers pay claims. Besides the contention by the insurance industry that it does pay claims, Gartner says it can't find independent evidence to confirm that. If you have significant cyber-insurance and experience a loss, Proctor says, you still may have a fight on your hands.



"Think this through with your insurance team to make sure you get appropriate coverage, and which ones pay."

Cyber-insurance is hot; more and more insurers see the potential of profits by offering cyber-insurance. It's risky for the insurers, and it's risky for the insured, too. Remember that when reviewing your cyber-insurance options. ■

http://www.inforisktoday.com/10-concerns-when-buying-cyber-insurance-a-4859

Case Study: Cyber-Insurance

Temple University Invests to Protect Assets

By Eric Chabrow

Lisa Zimmaro teaches insurance and risk management as an adjunct professor at Temple University, the state-supported school situated 1½ miles north of downtown Philadelphia.

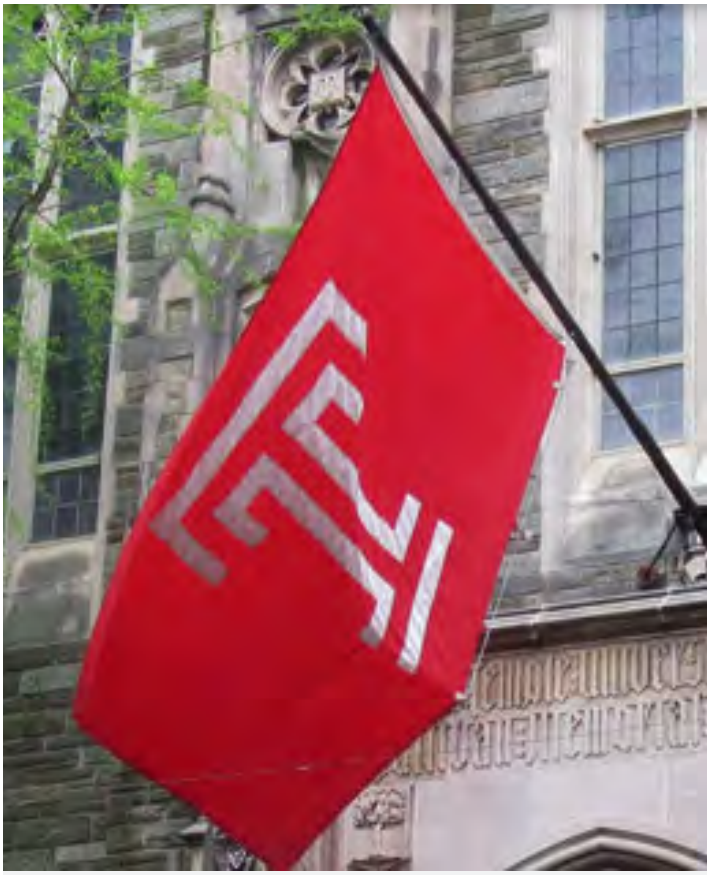
Her day job, though, gives her a lot of insight into cyber-insurance; Zimmaro is Temple's assistant vice president of risk management, whose responsibilities include buying insurance for the university.

Zimmaro says she first thought about cyber-insurance in 2008 after the university's chief information officer suggested such coverage. Two cyber-breaches in May and June 2009 turned her reflection into action. During a seven-week period in late spring 2009, the University of California at Berkeley and Cornell University separately revealed major security breaches, exposing the personally identifiable information of more than 200,000 students and alumni between both institutions. "Those two events pushed us over the edge," Zimmaro says. "They happened close enough together that it made us say, "'Okay, that's it.'"

It didn't take the nation's 27th largest university with an enrollment of 36,000 students long to act: In July 2009, with the help of Temple's insurance broker, the school acquired a cyber-policy from insurer Chartis, with coverage up to $10 million a year. In the 2-plus years since the policy took effect, Temple has yet to have had the need to file a claim.

To get the best policy, the school's broker approached 10 different carriers, and though some insurers may have offered a lower premium, price alone shouldn't be used to determine which policy to take. Not all policies offer the same protection, and reliability varies among insurers. Zimmaro thinks Temple's cyber-policy is worth the premium. She wouldn't provide an exact amount the university pays in premiums for cyber-insurance but furnished a range: $100,000 and $200,000 a year. Premiums could have been higher, but Zimmaro decided on a bigger deductible than the university takes on other types of liability insurance policies.

"I got boatloads and buckets of all types of insurance here at Temple; cyber is not making me cringe or throwing me over the edge, premium wise. It doesn't even come close to general liability or property insurance," Zimmaro says. "But what did push us toward this is that there are exclusions in general liability (GL) policies that made us think that had we had a breach, our general liability carrier would deny coverage, and a lot of GL carriers are doing that now because they don't want to be on the hook for a data breach."



"Those two [breach] events pushed us over the edge. They happened close enough together that it made us say, 'Okay, that's it.'"

- LISA ZIMMARO, TEMPLE UNIVERSITY

> **"I got boatloads and buckets of all types of insurance here at Temple; cyber is not making me cringe or throwing me over the edge, premium wise."**
>
> - LISA ZIMMARO, TEMPLE UNIVERSITY

Nearly Every Imaginable Act Covered

Simply, she says, Temple's cyber-insurance covers nearly every imaginable act that could have an impact on its IT systems, protecting the school from breaches caused by outsiders as well as those from insiders, whether or not their intent was to intentionally cause the university harm. The insurance covers Temple for consequences of a breach, such as credit-monitoring services for those whose personally identifiable information is exposed, as well as legal costs to defend the school against liabilities resulting from, say, exposure of sensitive data.

Edward DeMarco, director of operational risk and director of regulatory relations and communications at the Risk Management Association, says speaking with a knowledgeable broker is smart, but organizations - his association represents banks - should also seek out lawyers who are savvy and experienced in insurance coverage disputes to review policies. "If you got someone to read the policy, understand exclusion and sit and talk to IT people at a firm, you're really in a position to see if you're adequately covered or not," DeMarco says. "Otherwise, you're potentially taking a reputational hit. You may be subject to fines, depending on what the data is that's breached. Your stock price is going to go wonky, and sometimes you're going to lose confidence in management."

After the vetting process, qualifying for insurance can prove to be a tedious task when compared with applying for other types of liability insurance. Temple had to fill out a detailed, 30-page application, providing information about safeguards the school is taking to defend its data and systems. The CIO was interviewed by the insurer as well. Because Temple never had cyber-insurance, thus not having a history on claims the insurer might need to pay, more due diligence was required for the initial policy. In the future, Zimmaro believes renewal should be far less arduous, as is the case with other types of liability insurance, because a history on claims - or lack thereof - would exist.

The most important piece of advice Zimmaro offers on seeking cyber-insurance is to have a good, trustworthy broker, who not only understands the organization's needs regarding cyber-insurance, but can properly vet insurers. ■

---

http://www.inforisktoday.com/blogs/case-study-cyber-insurance-p-1126

When it comes to

We've got you covered.

News | Education | Research

BANK INFO SECURITY®
CU INFO SECURITY® (Just for Credit Unions)
GOV INFO SECURITY®
HEALTHCARE INFO SECURITY®

US | UK | EU | IN | Asia

infoRisk TODAY®

US | UK | EU | IN | Asia

CAREERS INFO SECURITY®

US | UK | EU | IN | Asia

Data Breach TODAY®
Prevention. Response. Notification.

US | UK | EU | IN | Asia

ISMG
INFORMATION SECURITY MEDIA GROUP

www.ismgcorp.com