THE DAILY RECORD

CYBER REPORT

2016

IN THIS ISSUE

TABLE OF CONTENTS

THINKSTOCK IMAGE

BUYING INTO THE BRAVE NEW WORLD OF CYBER INSURANCE

By Nick Stern
Special to The Daily Record

Most business owners whom Valerie Corekin comes in contact with don't think at first that the cyber insurance plan they're pondering is as crucial to their risk management strategy as life insurance is for their personal lives.

"Business owners who think that they don't have to secure their data and IT technology with the same level of due diligence they use to protect their physical assets, such as on a building, are not making good decisions," said Corekin, a senior risk advisor with PSA Insurance & Financial Services in the Washington D.C. metro area.

Digital exposure is much greater than people realize, instances of cyberattacks and breaches are growing, and so is the publicity surrounding them. "There are costs associated with this," she said. "Those costs are pretty scary, too."

According to the Poneman Institute's 2016 Cost of Data Breach study of 64 U.S. firms, the average lost or stolen "record" containing sensitive and confidential information cost $221 this year, up from $217 the year prior. This may not seem like a pricey sum until you consider breaches this year to organizations involved 29,611 records on average and companies shelled out an average total cost of $7.01 million to resolve cyber breaches, a number that has risen about seven percent since 2015.

BEFORE YOU BUY

But how do you choose a reasonable cyber insurance policy among the hundreds offered?

When Frank Giachini, senior vice-president of operations at PSA, looked at plan for his firm, his first consideration was determining the company's level of exposure. Ask yourself whether you can survive a temporary interruption or shutdown of operations or pay for the costs associated with, say, notifying exposed clients, he advised.

Evan Blair, cofounder and chief business officer with social media security and threat intelligence firm ZeroFox in Baltimore, said every business should

INSURANCE SEE PAGE 4

WHAT TO KNOW BEFORE YOU BUY A CYBER POLICY

Continued from **PAGE 3**

first conduct an audit and establish a written corporate security policy, wherein cyber insurance is included among various risk mitigation strategies as a sort of last line of defense. Make sure the policy looks to the potential impact—direct and indirect costs—a breach would have on your business operations, as well as how your customers could be affected, he said.

There are at least 47 different sets of state laws that regulate cyber breaches, Corekin said, so make sure you are knowledgeable about your company's potential responsibilities to secure its data. Some industries, such as health care, are highly regulated and have federal requirements that relate to electronic health care transactions.

Also, understand the precise limits of these policies and what steps have to be taken to maintain coverage—reputational damage from a high profile breach, for instance, could prove to be outside the scope of a recoverable loss, Blair said. "It's about trust and reputation at the end of the day with your customers."

COVERAGE NUTS AND BOLTS

Cyber insurance policies, which have only been around for over a decade, have many coverage options, but generally offer three buckets of coverage, Corekin said. These buckets can include: liability for security breaches when private information is released and costs for items such as regulatory compliance fees, legal issues or the expenses associated with unlocking the system after a hack. Also, the policies can cover business interruption expenses.

Note that most standard insurance policies, including business liability insurance, business interruption insurance, or even computer fraud coverage, will likely no longer cover the fallout from a cyberattack, Corekin said.

Another point of potential confusion: Understanding the precise meaning of the terms associated with a breach of privacy. Buyers can quickly stray into the weeds when trying to figure out the precise meaning of terms in the policies like "glitch" or "wrongful act," but knowledgeable agents will guide you through this, she said.

MORE TIPS

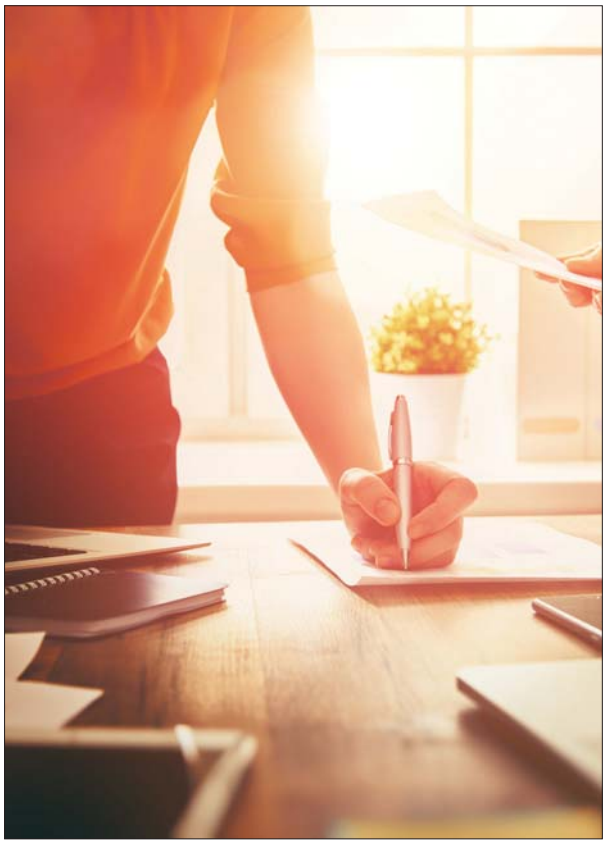
Before you buy, choose the right partner, Corekin said. Executives considering an insurance company should carefully weigh its experience writing cyber policies. For instance, you'll want a provider that has dedicated staff and resources surrounding cyber policies, Giachini said. And make sure your agent understands the types of policies on the market and is conversant in the relevant terminology. Smaller or regional carriers could be fine for some companies, while national players with a larger pool of resources may be preferable for others, he said.

If your firm operates around the clock and a breach could affect operations at any time, you'll need a provider that will pick up the phone on a Friday or Saturday evening, Corekin said. In some states, you may only have 72 hours to meet regulatory deadlines to respond to a breach.

Nail down your cyber risk mitigation strategy in a holistic fashion, Blair recommended. For example, small businesses should look into cloud security that provides relatively inexpensive and hands-off cyber defense.

Establish acceptable use policies for employees that also spell out disciplinary actions for failing to follow protocols, Giachini said. Focus too on educating staff members about the latest risks from attacks and make sure all software is updated with new patches.

Finally, to connect with cyber experts and professionals to assess your security plan, reach out to the nonprofit Cybersecurity Association of Maryland, Inc.



THINKSTOCK IMAGE

OBLIGATION TO PROTECT CLIENT DATA FOUND IN LAW, ETHICS RULES

By Heather Cobun
Heather.Cobun@
TheDailyRecord.com

MAXMILIAN FRANZ/THE DAILY RECORD

Maryland law requires a business to have reasonable security measures in place, said Howard R. Feldman, co-chair of the cyber security and information privacy group at Whiteford Taylor Preston LLP in Baltimore.

A basic understanding of technology is more than just good business for law firms: it's increasingly becoming an ethical obligation.

As of September, 25 states have adopted some kind of duty of technology competence and the American Bar Association amended a portion of its model rules in 2012 to require attorneys to keep abreast of the benefits and risks associated with relevant technology.

In states where there is no express rule, portions of existing ethics rules can be read to place certain responsibilities on law firms from the hardware they employ to their email server, according to C. Bernard Eydt, attorney and CEO of Pryvos, a cyber security consulting firm with offices in Maryland and New York.

Most ethics opinions from around the country say the responsibility to protect client data derives from rules that have been around for decades, including those pertaining to competence, communication and confidentiality, Eydt said.

"It's gotten more attention," he said. "It's probably more likely that as attorneys get hacked, they recognize these issues."

In addition to ethics rules, many states have statutory obligations for any business handling personal information, including law firms, according to Howard R. Feldman, co-chair of the cyber security and information privacy group at Whiteford Taylor Preston LLP in Baltimore.

> "Because schemes and technology are advancing at an ever-changing pace, you should revisit your policies annually."
> **Howard R. Feldman**, co-chair of the cyber security and information privacy group at Whiteford Taylor Preston LLP in Baltimore

"Law firms are no different than any business," he said.

Maryland's law is flexible and requires a business to have reasonable security procedures in place to prevent unauthorized access or disclosure of personal information, but other states, like Massachusetts, have more specific guidance, according to Feldman.

In general, the laws allow for businesses to take steps that are proportional to their size and budget.

"A ma and pa store can't afford to have every bell and whistle security procedure in place," he said, but added "you can't do nothing, either."

It's becoming more common for larger companies to have chief privacy officer who oversees protection of client data, according to Feldman, but small businesses should not consider themselves excused from the requirements if they can't afford a full-time staff member dedicated to cyber security.

"A lot of businesses, this isn't even on their radar screen either because they think they're a small target or not a target," he said. "Small companies can be a target, so you can't assume."

BASIC STEPS

According to Towson attorney and self-described "tech guy" Adam M. Spence, the rule is "reasonable care" when dealing with client data.

Basic steps can be taken by attorneys from small or large firms to avoid becoming an easy target for a hack, according to Spence, who recommends having unique passwords for every program and device with a login as well as not using public wireless networks to access confidential documents.

The vast majority of hacks are initiated through email scams, Spence said, so having a firm policy in place against clicking links and opening attachments from unfamiliar sources can also go a long way to prevent an attack.

"Unless it's from a trusted source that you're expecting, don't open it," said Spence of Spence|Brierley PC. "If there is doubt, then you don't do it... You can shut down your system."

Eydt said the biggest change in recent years for attorneys is the growing need to encrypt email as the reasonable expectation of privacy in such communications

"Today there's not a requirement, but as more and more people have access to unencrypted email and unencrypted data, some people could say you've breached your professional responsibility," he said.

Spence said there are websites that offer a secure interface for email as well as software, though both sides need to have the software installed. For additional security, documents can be protected with one or multiple passwords.

Feldman said it's also important to frequently train employees and revisit policies.

"Because schemes and technology are advancing at an ever-changing pace, you should revisit your policies annually," he said.

A firm unsure of what reasonable steps to take can ask a knowledgeable company to come look at their systems and make practical suggestions on good security measures.

MAXMILIAN FRANZ/THE DAILY RECORD

Many of the students pursuing degrees in cybersecurity at the University of Maryland Baltimore County are already working in the field and are looking to further their knowledge or advance their careers.

TEACHING FOR THE REAL WORLD

Area colleges advance their cyber programs

By Gina Gallucci-White
Special to The Daily Record

MAXMILIAN FRANZ/THE DAILY RECORD

A lot is already in place to educate workers for today's cybersecurity market, but those efforts must continue, Stacey Smith, Cybersecurity Association of Maryland's executive director, said.

With the National Security Agency, United States Cyber Command, Defense Information Systems Agency and the National Institute of Standards and Technology all within the state's borders, Maryland has become the epicenter for cyber security that politicians once predicted.

In fact, the National Initiative for Cybersecurity Education recently released an interactive job supply and demand heat map: Maryland was one of eight states with the highest demand for cyber security jobs. Others include Virginia, Texas, California and New York. While demand is high in these areas, the map noted supply of workers is low with nearly 350,000 jobs available in the field across the country.

Stacey Smith, Cybersecurity Association of Maryland's executive director, said companies that have cyber positions to be filled will tell you there is a need for a more skilled workforce. Some academic institutions and programs are working on creating internships and apprenticeship opportunities to get the younger generation some real world experience to bring to the companies in Maryland.

"The problem is only getting greater and therefore there is even more of a need for businesses to be focusing their efforts on the security of their business or their government agency or entity," she said. "I do think Maryland is doing some really great things and continuing to generate a really skilled and talented workforce. One of our biggest assets is our people that we have here. With the academic institutions, with the programs that the private sector have with some of the government agencies and training efforts together, I think that we've got a very skilled workforce and we need to continue to put our efforts toward making sure that we always do."

Many local colleges and universities have created undergraduate and master's degree courses to prepare students and turn them into qualified professionals ready to handle and protect important cyber data. And many of these students are already in the workforce – some work in information technology while others are already in cyber security.

"They are coming to the University of Maryland, Baltimore County for promotion potential and they want to brush up on their knowledge, their professional skills and advance their career," said Dr. Richard Forno, director of UMBC's cyber security graduate program. "Not many of my students are looking to break into the field out of the blue. They are already in the field doing something with cyber but we are seeing more younger students, recent college graduates who want to continue in their education and move into cyber. That demographic is shifting a little bit. It used to be all professionals, now we are seeing a mix of professionals and younger folks."

The University of Maryland University Campus has around 12,000 students earning bachelor's and master's degrees and certificates in cyber security. "What we are providing is a state of the art curriculum that is based on real world scenarios and techniques and hands-on tools used in today's organizations so we are looking at 'What are the skills, abilities and competencies that are needed by companies to actually get their job done' when it comes to cyber securities," said Dr. Emma Garrison-Alexander, UMUC's vice dean of cyber security and information assurance. "How do they protect their investments? How do they protect their assets? How do they protect the data that is very sensitive and that they want to keep protected? So our curriculum is matched up to what is needed in the real world. ... We are preparing students with the cyber security knowledge and skills that are immediately applicable to the work environment."

Many UMUC cyber security professors are working in the field including as chief information security officers, engineers and cyber analysts. "When they come into the classroom, they are not just teaching theory," she said. "They are actually teaching the curriculum in a way that has direct applicability to the real world."

When UMBC created their cyber security program nearly a decade ago, they consulted local government and private sector employees about the qualities and ideal job candidates they would like to see come out of their program. "The top four or five things they told us they wanted had nothing to do with cyber," Forno said. "They wanted people who could communicate, work well in teams, work well with others, (and) write well ... so we structured our program in a way that took that into account so it provided a mix of both the cyber skills for professional but those soft skills to put that knowledge into practice effectively."

While UMBC does not track graduate placements, Forno said he has seen some United States Army personnel complete the graduate program and be assigned directly to nearby Fort Meade. "We are preparing them for that role they are being groomed for," he said.

Others have gone on to jobs in the private sector and government offices. UMUC has also seen their graduates prosper after graduation.

"We are not just about teaching students what they should know about cyber security, but we are also teaching them in such a way that they are gaining skills that they are going to be able to use in the workforce that are directly transferable from the classroom to the work environment," Garrison-Alexander said.

THREAT INCREASES FOR HEALTH CARE HACKS, HOSPITALS RESPOND

By Meg Tully
Special to The Daily Record

THINKSTOCK IMAGE

Maryland cyber security experts are stepping up to protect hospitals, healthcare offices and agencies as stolen medical records are becoming more valuable in today's economy.

"The bad guys are no longer just trying to hack into the Pentagon, they are trying to attack your medical records and your credit cards," Michael Ryan, CEO of Annapolis-based South River Technologies, said. "That information is just as critical."

As such, hospitals must take the need for secure file transfer seriously, Ryan said. Just a few years ago, major healthcare institutions were still relying on non-secure formats like email for file transfers, he said.

South River partners with hospitals and larger medical facilities from all over the world, as well as financial institutions, to make sure data can be shared securely without relying on email. The company's primary product, Cornerstone MFT, allows doctors and nurses to collaborate in real time on patient files on a secure server.

One rising threat Ryan has seen is a ransomware attack, in which hackers attack a hospital, infect the system and encrypt all the patient information. Hospitals are contacted to pay a ransom in order to that data back – but in some cases, they pay amounts like $40,000 and never regain the data.

Because of that, South River's product line includes an offsite suppository to mirror data in a HIPAA compliant manner. The company also works with clients to prevent attacks, address threats and stay on top of the latest technology.

A MARKETPLACE OF ITS OWN

Cybercrime has its "own ecosystem now. It's in its own unique marketplace," said Jon Burns, senior vice president and chief information officer for the University of Maryland Medical System. "Health care data is ten times the value of credit card data and the value of health care data is greater than what it would have been ten to fifteen years ago."

Many in the health care industry worry that stolen medical data could be used to perpetrate Medicaid or insurance fraud. Unlike credit card breaches, which are often caught quickly and resolved with the issuance of a new card, medical data breaches are not a one-time event, Burns said. The stolen data could be used repeatedly.

The cost of protecting data, patients and employees has become the new cost of doing business and ongoing one.

"You can't implement a series of technology and be done," Burns said.

At University of Maryland Medical Center, prevention includes annual employee training, monthly security council meetings with the cyber team, compliance officers, auditors and physicians, as well as regular consultations with an cyber expert, a former CIA employee. The hospital also has a good relationship with the FBI's cyber security task force in Baltimore, Burns said.

The hacking threat to health care differs from other industries because health care has so many digital systems and because patients are involved, said Darren Lacey, chief information security officer for Johns Hopkins Hospital. A breach in a manufacturing plant, for example, may not have the impact on people that a hack resulting in stolen medical records would.

> "There's nobody who's naturally thinking about the space in between."
>
> AJAY K. GUPTA,
> CEO OF THE ROCKVILLE-BASED NONPROFIT, HEALTH SOLUTIONS RESEARCH, INC.

Still, Lacey said, hospitals pay more attention to technology than ever before and that is a good thing.

"In terms of overall awareness and visibility, cybersecurity is in so much better shape than it was five years ago, and that's given me reason to be optimistic," Lacey said.

SECURITY VS. ACCESS

While cyber experts are always thinking about security of data, patients are often thinking more about access. "There's nobody who's naturally thinking about the space in between. Sometimes we want data secure and sometimes we want it open and accessible in the case of emergency. Having your data does no good if the physician and the EMS treating you can't read it," said Ajay K. Gupta, CEO of the Rockville-based nonprofit, Health Solutions Research, Inc.

In the case of an emergency, patients want first responders and physicians to be able to access secure patient portals, according to a study which HSR presented last year at the Aging in America conference. This kind of access would allow responders to have knowledge of past medical and surgical history, life-threatening allergies or other information that could save the patient's life.

But how that data would be accessed would vary. HSR has proposed that EMS workers be able to use a person's fingerprint to access a mobile app. Another solution would be to plug in an emergency code that could be entered into a secure system and perhaps accessible on a medical ID bracelet worn by the patient, Gupta said.

Still, access should not be considered without security, he said, noting that medical records can be used for identity theft, bank account theft or even as fake medical histories for immigration applications.

CYBER IN A MOBILE WORLD

Because today's medical workforce is increasingly connected through mobile devices, cyber policies and procedures must reflect that, said Gina Abate, president and CEO of Edwards Performance Solutions in Elkridge.

For instance, Edwards recently recommended that a large healthcare agency improve the authentication process for key access points when employees telecommute, and developed a tutorial for employees. Since implementing the process agency-wide in January, there have been no breaches.

"In this day and age it happens to companies of all sizes," she said. "You need to understand what your cyber risks are and as a business you need to make an educated decision about what risk you can accept and what risks you can take action on."

YOU CAN'T BUILD THE BUSINESS OF TOMORROW ON THE NETWORK OF YESTERDAY.

It's no secret: business has changed—in every way, for every business. Modern technologies have brought new opportunities and new challenges, like BYOD and a mobile workforce, that old networks just weren't built for. While demand on these networks has increased exponentially, networking costs have skyrocketed and IT budgets haven't kept pace.

Comcast Business Enterprise Solutions is a new kind of network, built for a new kind of business. With $4.5 billion invested in our national IP backbone and a suite of managed solutions, Comcast Business is committed to designing, building, implementing and managing a communications network customized to the needs of today's large, widely distributed enterprise.

INTRODUCING COMCAST BUSINESS ENTERPRISE SOLUTIONS

COMCAST **BUSINESS** B4B BUILT FOR **BUSINESS**™

business.comcast.com/enterprise