Advisen
Transforming • Insurance℠

UNLOCKING THE VALUE IN CYBER DATA:
GETTING A CLEARER VIEW OF RISK

Sponsored by

PIVOTPOINT
RISK ANALYTICS

January 2016

ACCORDING TO JULIAN WAITS, PRESIDENT AND CEO OF PIVOTPOINT RISK ANALYTICS, THE KEY IS TO DETERMINE THE ASSETS THAT MUST BE GUARDED MOST RIGOROUSLY – AND WHAT THE CONSEQUENCES WOULD BE IF THEY WERE ACCESSED BY THE WRONG PARTY.

As commonplace as cyber attacks and data breaches have become, the process of evaluating the cyber risk of an organization – as well as underwriting and pricing cyber liability coverage – has been described as a guessing game. Policyholders and insurers alike hope the number they settle upon will accurately reflect the risk insured.

The typical lament among the industry has been that the cyber insurance marketplace is too new, too untested, and backed by too little data to make much more than an educated estimate on the right price. More data must be collected to mirror the time-honored underwriting processes of other lines of business, say experts.

However, insurers, brokers, and their clients may already be able to determine their risks and potential for cyber losses. Just as a home insurer evaluates the structure of a dwelling, its construction, its proximity to perils, and its contents, organizations – and their insurance partners – have the chance to determine what the ramifications of a cyber event could be by examining their data and the security structure protecting it.

Every organization in every industry faces cyber risk. A critical infrastructure operator might be concerned about physical damage to its control systems, a healthcare provider might worry about the sensitive personal health information of its patients, and a retailer would need to think about payment card data being breached. Assets carry value for organizations, but they can become a liability since they pose a tempting target for cybercriminals.

For organizations, concerns over cyber risk have risen to the top, according to a recent survey from the Depository Trust & Clearing Corporation (DTCC), which found that 77 percent of North American risk managers identifying the risk as a top-five worry. One respondent to the survey commented, “Cyber risks appear to be multiplying while controls to address these risks may not be able to keep up with the continually escalating threats.”

A recent survey conducted by Advisen and Zurich also found that 92 percent of executives view cyber risk as at least a “moderate threat” to their organizations but addressing the risk leaves them with a sense of helplessness.

“It’s a growing concern, but limited resources to address leave us vulnerable,” said respondent to the survey. “I continue to raise the issue. Coverage continues to develop.”

For those risks not mitigated in other ways, cyber insurance more readily appears to be a solution to more organizations, but the question becomes “How can organizations determine whether their cybersecurity investments are properly deployed and their insurance programs are as effective as possible.

IDENTIFY – AND PROTECT – THE CROWN JEWELS

It all comes down to estimating the potential financial impact of a cyber event. According to Julian Waits, president and CEO of PivotPoint Risk Analytics, the key is to determine the assets that must be guarded most rigorously – and what the consequences would be if they were accessed by the wrong party. Organizations must also evaluate the effectiveness of their own cybersecurity posture with an eye toward the segments of business that needs the most protection.

Waits commented, “You have to know what you’re insuring and what you’ve been doing from a maturity perspective.”

Imagine your organization has 100 applications across the operation. If breached, 80 of those applications are likely to rise to a “nuisance” level, but do no real harm to the organization’s reputation or financial stability. The remaining 20 applications, however, have the potential to create significant damage, be it financial or physical.

PivotPoint has launched a tool called CyVaR, which measures “cyber value at risk,” and seeks to understand the nature of their business and its vulnerabilities to hacking or accidental breaches, according to Waits.

“We take an inside-out approach,” he said. Waits added that he starts from the perspective that every organization will at some point be hacked – building the resilience to recover from a breach becomes the goal.

Waits highlighted the value in examining the “known liabilities” within an application – a point-of-sale system, for example, has the risk of losing payment card data. However, looking purely at the data contained within an application does not present a full picture of the risk.

“We believe that’s only one variable,” he said. Looking at the number of records held doesn’t take into account cost of notifying consumers, or the cost of settlements, or the loss of trust that results in loss of customers. Waits advised evaluating the costs associated with legal fees and settlements and looking at the probability of an attack through the use of threat data.

“We make the assumption that you will be breached at some point,” said Waits. “If the bad guys are persistent enough, they’re going to get through. So then the question becomes, where am I most likely to be breached, and how much would that breach cost my organization?”

IMPERATIVE TO PROTECT DATA

Organizations now have an imperative to protect the data that has been entrusted to them, as well as securing their digital borders against business-interrupting intrusions. The legal landscape regarding accountability for data breaches continues to develop, but it has become clear that regulators, lawmakers, and the public will hold the breached entity responsible for a cyber event and the loss of data. This trend means that a cyber event of any type has the potential to negatively affect an organization’s revenue and reputation.

An organization’s major risk might not be data, according to Lon Berk, attorney with Hunton & Williams LLP. It might be physical damage from a cyber event, or disruption in operations, or disruption to the industrial control systems. The exposure varies by industry, as does the risk of attack.

AN ORGANIZATION’S MAJOR RISK MIGHT NOT BE DATA, ACCORDING TO LON BERK, ATTORNEY WITH HUNTON & WILLIAMS LLP. IT MIGHT BE PHYSICAL DAMAGE FROM A CYBER EVENT, OR DISRUPTION IN OPERATIONS, OR DISRUPTION TO THE INDUSTRIAL CONTROL SYSTEMS.

Understanding that an organization must protect its data and where the most critical assets reside means that a company can deploy its security and insurance budget in the most effective way, according to PivotPoint’s Waits. It can also demonstrate to boards, shareholders, and insurers that an organization has sought to reduce its risk.

“If a company is relatively immature on security, we can walk them through our business impact analysis,” Waits said. Clearly

identifying the most significant sources of risk can streamline communication between a chief information security officer and management and illustrate a return on investment for security efforts.

VALUE FOR INSURERS

That determination, that information has myriad levels of importance for organizations. It also holds value for insurers. Unlike many lines of coverage, where insurers have decades of loss data to tell an insured exactly what their property or casualty premium should be and how much coverage they should carry, the cyber market has not matured to that level. Who should be responsible for making these decisions? All involved, say experts.

"It's two sides to the same coin. Companies clearly have to be able to get better at understanding the size of the risk they have," said Ben Beeson, broker at Lockton Companies. "On the other side, the insurance industry has to be able to quantify it themselves to be able to price."

With a shortage of historical data, insurers and brokers have turned both to predictive analytics and educated guessing.

"It's crude. Anyone who tells you otherwise in the broker community, I'm not sure they're telling the truth," Beeson said. "It's a bit more of an art than a science at the moment."

Every insurer has its own approach and appetite for underwriting, but industry standards and risk models exist for most lines of business. Cyber offers a ripple in those industry waters since it is not only a nascent risk, but a rapidly changing one. The threat environment faced by organizations evolves every day, with cyber criminals and hackers dedicated to finding the next best way to crack security measures.

"How do you model such a dynamic risk environment?" Beeson asked. He predicted a shift toward incorporating cyber threat information into predictive models.

"You're going to see a convergence between companies who can provide real-time data feeds," he said. "It will drive more capacity in the market, which we badly need."

The insurance industry has been building its expertise in cyber for over a decade, but different companies take different views on the data that will best depict clients' probable cyber losses. Some might focus on whether a company encrypts all its data, or follows the National Institute for Standards and Technology's (NIST) cybersecurity framework.

"I don't know if there's a uniform notion of what to insure in the industry," said Berk, who assists clients in placing their insurance programs.

"The risk factors are constantly changing," said Emy Donavan, national practice leader for Allianz Global and Corporate Specialty (AGCS). "The more that we see the risk evolving, the sort of data that we consider problematic is changing. Sony taught us that."

MOVING RISK TARGET

Insurers – and their clients – are now beginning to look at the type of attacks that an organization might experience. Hacking has evolved, shifting from personal attacks on organizations to stealing customer data for online black-market use, back to personal attacks. As attacker motivations change, companies must realize that an

AS ATTACKER MOTIVATIONS CHANGE, COMPANIES MUST REALIZE THAT AN OFF-COLOR JOKE MADE IN AN EMAIL FROM ONE EXECUTIVE TO ANOTHER, FOR EXAMPLE, MIGHT HAVE THE POWER TO DAMAGE A COMPANY'S REPUTATION, EVEN IF NO PERSONAL DATA HAS BEEN LEAKED AND MONETIZED BY CRIMINALS.

off-color joke made in an email from one executive to another, for example, might have the power to damage a company's reputation, even if no personal data has been leaked and monetized by criminals. Any leak of such emails, by a disgruntled employee, a hacker, or an unintentional error could expose a company to embarrassing and costly litigation.

"It's a little bit of a moving target," said Donavan. "I think at some point there will be standardization of the sort of attacks that happen and eventually we'll have a better sense of how much that will cost."

Even after just five or so years of frequent data breaches, insurers are better able to estimate the costs of notifying affected consumers and pinning down legal fees for the process. With another five to 10 years of data, "barring any crazy curveballs," the insurance industry and its clients should be in an even better position to estimate losses.

EXPERTS AGREE THAT NO ONE SOLUTION WILL RESOLVE ANY ORGANIZATION'S CYBER RISK, BUT COMBINING TECHNOLOGY AND INSURANCE CAN MAKE SIGNIFICANT STRIDES TO IMPROVING THE CHANCES THAT AN ORGANIZATION CAN MORE QUICKLY BOUNCE BACK FROM A CYBER EVENT.

SOLVING THE PROBLEM

Experts agree that no one solution will resolve any organization's cyber risk, but combining technology and insurance can make significant strides to improving the chances that an organization can more quickly bounce back from a cyber event.

"Every technical solution has a flaw, so the pendulum is swinging. Insurance isn't the answer alone and technical solutions aren't the answer alone. There's a complicated cost-benefit analysis," said Lon Berk, attorney with Hunton & Williams LLP.

"Think about the data that's at risk for your industry," said Berk. Understanding that data that your organization holds – and what it needs to keep and to eliminate – presents a better view of the risk both for the organization and an insurer underwriting and pricing a risk.

"A lot of clients don't even have that level of understanding of their own risk. A lot of it is about education," said AGCS' Donavan. She explained that many potential insureds are "shocked" at the questions asked for cyber coverage – and are equally surprised when insurers decline their applications. Insurers themselves now seek to find the right questions to ask to determine an insured's level of preparedness for cyber risk.

Many industry observers question whether cyber insurance applications accurately capture a snapshot of the risks being evaluated. Depending on an organization's internal structure, the individual procuring insurance may not be the best person to report on the cybersecurity processes, or the application may not take into account all exposures. While the underwriting process improves, more emphasis can be placed on understanding value at risk.

WAITS POINTED OUT THAT MOST ORGANIZATIONS HAVE "DORMANT" CYBER RISKS ALREADY LURKING ON THEIR SYSTEMS WITHOUT THEIR KNOWLEDGE AND AN EVENT IS LIKELY TO OCCUR SOONER AND MORE FREQUENTLY THAN A HURRICANE, FOR EXAMPLE, OR OTHER CATASTROPHIC RISKS THAT INSURANCE IS MEANT TO ADDRESS.

"It's a conundrum, but I think it's one that a lot of people are working on," Donavan said.

WHO SHOULD HARNESS THE DATA?

As cyber incidents occur, information about the type of threats experienced, the organizations that fall victim to them, and the costs associated with the event can be collected by insurers, brokers, lawmakers, consulting firms, and technology vendors. It falls to all of those parties to find a solution that will harness the power of understanding that rests with the data and use it to more effectively secure networks. The insurance industry and the technology world have a "unique opportunity" to help organizations defend themselves and understand their risk.

"We should strive to be the industry that answers these questions," said Lockton's Beeson. "Insurance is right at the forefront. It's a bit of a level playing field and that's the good thing about cyber. It's a bit of a gold rush."

Time is undoubtedly of the essence in terms of taking advantage of the information that businesses have already gathered about cyber risk. Waits pointed out that most organizations have "dormant" cyber risks already lurking on their systems without their knowledge and an event is likely to occur sooner and more frequently than a hurricane, for example, or other catastrophic risks that insurance is meant to address.

"It's like going to a casino, nine times out of 10, the house is going to win," said Waits. "The liabilities are becoming so large."

The insurance industry may hold more pieces to the puzzle than it currently provides. In the approximately 15 years that cyber insurance has been developing, claims data has been collected and analyzed. Many observers feel that the information should be more widely shared to reveal trends and to provide insight into potential future losses.

"They view it as their competitive advantage," said Waits. He advised partnering across the industry, sharing loss data, and developing standards for underwriting and estimating losses.

Berk agrees that the insurance industry holds more useful data than may be being utilized now.

"Everybody complains about the data," he said. "But when you think about it, somebody has to have been collecting this data for 15 years. And

technology has been out there, and these cyber policies came out of tech E&O [errors and omissions]."

Crime and fidelity coverages could also offer insight into the frequency and severity of insider threats, such as employee theft. There has been a joint effort with the federal government and industry partners to assess and improve the state of the cyber insurance market as well as promote better cyber risk management for organizations. Tom Finan, former director of the Department of Homeland Security (DHS) leads the National Programs and Protection Directorate (NPPD) to build a repository of cyber data for use by both businesses and insurers.

Finan wrote in a paper earlier this year, "Conceptually, such a repository would aid insurers in delivering policies, at lower rates to 'best in class' clients – thereby contributing to and effectively informing the overall corporate risk management strategies of those clients. Such a repository also would support a host of advances for cyber risk management professionals, including enhanced cyber risk data and trend analysis, bolstered in-house cybersecurity programs, and improve cybersecurity solutions, products, and services."

Insurers do have claims data, but sharing it in a usable form might prove challenging. Allianz' Donavan explained that information systems at most insurers do not parse down to the exact type of loss in the cyber line, meaning there is a great deal of granular information, but it is not automatically illustrative in terms of trends.

"It's a question of how to extract that. It's not a lack of willingness," she said. Competitive advantage also comes into play for insurers that have focused on analyzing their own data to underwrite and price cyber right.

"There are a lot of companies that have eaten their shirts trying to get this right," said Donavan. "The more information that can be shared, the happier we'll all be."

CASE STUDY: CITY OF SAN DIEGO

When it comes to determining what type of data an organization must protect, the answer usually comes down to a few significant "crown jewels" that take the highest priority. For a municipality, every level of government can be open to cyber risk, from tax revenue to utilities and infrastructure to payment card data and health information for city workers. Gary Hayslip, the chief information security officer for the City of San Diego, discussed with Advisen how the eighth-largest city in the country found a handle on its cyber risk.

"When you deal with a city environment, politics is everything," said Hayslip. In explaining the risk and the value of the data that the city holds, he noted, he has focused on educating city leaders on the concept of taking "reasonable care" to protect data – data that includes point-of-sale systems, health data, municipal bonds and more.

"The city is a $4 billion business with 1.5 million citizens," Hayslip said. "It can get really, really ugly if you get a bad breach."

Hayslip worked with PivotPoint Risk Analytics to understand how analyzing the data could offer an outline for risk management for San Diego, a self-insured entity. The process allowed the city to pinpoint the top applications and better plan its resources for cybersecurity as well as factor the cost of preparedness into future development.

"We've got 24 networks, 11,000 users, and there's risk involved in that and we need to know about it," said Hayslip. San Diego has been able to put in place controls that enable the city "to absorb that attack, so we don't go down as a city."

Hayslip and the city of San Diego worked with PivotPoint to analyze five business applications that both generate

revenue and are critical to protection of the citizens. Through the CyVaR process, they ran a simulation with realistic threats to determine the value-at-risk for each of the five applications. Based on the results, the City received recommendations for specific actions to reduce its risk, such as implementing security frameworks produced by the Center for Internet Security (CIS) and the National Institute for Standards and Technology (NIST). CyVaR also gave Hayslip and his team insight into the potential costs of a breach and the "full risk exposure" of a breach.