accenture

CYBERSECURITY AT A PREMIUM

Are insurers staying ahead of their growing cybersecurity risks?

Accenture State of Cyber Resilience in Insurance

Contents

01

Introduction

In our last report about the insurance industry's ability to be resilient and bounce back quickly from cyberattacks, we noted a bit of overconfidence in executives' responses to our survey.

For example, about 80 percent of them indicated that they were either "confident" or "extremely confident" in their cybersecurity capabilities. Yet, the actual cybersecurity performance numbers did not support that position. Over twenty percent of attacks on their companies had resulted in breaches, and almost half of the firms surveyed required more than a week just to detect a problem, and even longer to remediate it. We hypothesized that insurance companies were buying time. They were being successful... for now. Cyber criminals were more focused on banks than insurers, but that situation would not last forever, we said.

Our latest findings, based on Accenture's 2019 "State of Cyber Resilience" report, those fears appear to have become a reality. The number of cyberattacks on insurers has more than doubled since our last survey (from 240 to 519 attacks, on average). This number is more than twice as much as the cross-industry cyber resilience leaders in the survey and over three times more than their banking/capital markets (CM) peers. When it comes to insurance and cybercrime, it's clear that the "bad guys" are paying attention.

Our research finds, however, that a group of insurance leaders are demonstrating far greater effectiveness at cybersecurity and cyber resilience than their peers. Emulating these leaders—not necessarily their level of investment but rather how they allocate those investments—is important to insurers' ongoing cybersecurity effectiveness.

First, the good news

The good news for insurance firms is that, although the total number of cyberattacks is up among surveyed respondents, successful breaches are actually down 42 percent since our last study—52 breaches on average before, 30 breaches now. Based on 519 total cyberattacks, that's a breach rate of 5.8 percent. (The breach rate for cross-industry cyber resilience leaders was even lower, at 3.8 percent.) Banking/CM, by contrast, had fewer attacks but more breaches on average—an 11 percent breach rate.

More positive indicators: In our last cyber resilience survey, only 9 percent of insurers could detect a security breach within 24 hours. In this survey, 32 percent of insurance firms have that capability. Last time, we found that just 33 percent of insurers could remediate a breach in 30 days or less. That number is up to 72 percent now.

As cyber criminals increasingly profit by selling their software to others, the toolsets used by attackers have been commoditized. Although this has driven up the number of attacks, many insurers have improved their ability to fend off this "nuisance" variety. They've also gotten better at insisting upon more complex passwords and two-factor user authentication on things like webmail. These tactics are effective at stopping a great number of attacks.

Another catalyst for change is the growth in the number of insurers entering the cyber insurance market. By doing so, they are raising their knowledge and awareness of what it takes to be cybersecure, and that's causing them to improve their own internal capabilities.

Indirect attacks are on the rise

A closer look at the sources of cyberattacks among "State of Cyber Resilience" respondents reveals that 40 percent of insurance firms' security breaches are now indirect—meaning, via a third party connected to the company's network—as threat actors target the weak links in the supply chain or business ecosystem. These exposures can take an explicit form like the injection of malicious code into a vendor's site, downloaded open-source libraries or a vendor's misconfigured server. They can also use access to a third party as a means to attack the insurer.

Organizations should look beyond their four walls to protect their business ecosystems and supply chains. On average, according to our survey, cybersecurity programs actively protect only about 55 percent of an insurer's organization (much lower than global, cross-industry leaders, where 80 percent of the organization is actively protected).

That is an issue when 40 percent of breaches come via this route. Indirect attacks are particularly difficult to control as companies are increasingly relying on a remote workforce. It is challenging to monitor such a workforce—especially one located across multiple companies—to check that everyone is compliant with encrypting Wi-Fi, changing passwords regularly, running the required monitoring software and staying vigilant about phishing attacks and other threats.

Internal organizational boundaries and roles also play a part in delaying companies' maturity in stopping indirect attacks. In some cases, detecting and stopping indirect breaches at a subsidiary are not clearly within anyone's particular jurisdiction, so performance goals and metrics may not be in place. It can be tempting to pin a breach on a subsidiary's security exposure, but in the long run, that doesn't really help the parent company extricate itself quickly from the effects of a breach, whatever its origin.

On average, cybersecurity programs actively protect only about 55% of an insurer's organization.

Insurance firms experienced fewer breaches, but are not recovering quickly enough from successful ones and are exposing more customer data.

As noted, insurers experienced fewer cybersecurity breaches than in our last survey. On the other hand, they are lagging in other areas:

56%

Low detection rates:
83 percent of breaches among cross-industry cyber resilience leaders are found by security teams, but only 56 percent of insurers' breaches.

6%

Long-lasting breach impacts:
Among cross-industry leaders, 45 percent say all breaches had a business impact of less than 24 hours. Only 6 percent of insurance companies could say the same.

44%

High levels of customer data exposed:
44 percent of insurers had more than 500,000 records exposed in the last year, compared with only 15 percent of cross-industry leaders.

Investments are up, but firms worry that, over time, they won't be able to keep pace.

Finally, surveyed firms are investing in cybersecurity at higher levels according to our survey. Additionally, 89 percent of insurers spend more than one-fifth of their cybersecurity budgets on advanced technologies (e.g., artificial intelligence, machine learning and robotic process automation), up from 68 percent three years ago.

But one senses a certain resignation, if not futility, about how much high-end cyber protection costs, and what it is expected to cost in the future. Sixty percent of insurance respondents report that costs for cybersecurity protection have grown over the past two years, and about one in five (22 percent) say that those increases were more than 25 percent. Overall, 72 percent of insurance institutions indicate that staying ahead of attackers is a constant battle and that the cost is ultimately unsustainable.

02

How cybersecurity insurance leaders stand out

02 HOW CYBERSECURITY INSURANCE LEADERS STAND OUT

Detailed modeling and statistical analysis of cybersecurity performance has identified a group of insurance leaders that are at a significantly higher level of performance compared with the non-leaders. Accenture's statistical analysis revealed that the performance of insurance cybersecurity leaders exceeds their peers in four areas in particular. They:

Stop more attacks **Find breaches faster** **Fix breaches faster** **Reduce breach impact**

The disparity between the performance of cyber resilience leaders vs. non-leaders was quite pronounced (See Figure 1.)

Figure 1. Better performance among insurance cyber resilience leaders

Characteristics	Leaders (8%)	Non-Leaders (83%)
Stop more attacks	**3%** of breaches are successful	**14%** of breaches are successful
Find breaches faster	**88%** detect breaches in less than one day	**26%** detect breaches in less than one day
Fix breaches faster	**97%** fix breaches in 15 days or less	**37%** fix breaches in 15 days or less
Reduce breach impact	**53%** of breaches have no impact	**24%** of breaches have no impact

Source: Third Annual Accenture State of Cyber Resilience Survey

02 HOW CYBERSECURITY INSURANCE LEADERS STAND OUT

Insurance leaders excel in other areas, as well. For example, cybersecurity capabilities protect 82 percent of leaders' organizations but only 52 percent of non-leaders' organizations. In addition, insurance leaders' security teams discover 81 percent of all breach attempts, while non-leaders' teams discover just 55 percent. The more issues discovered by internal security, the less chance that such issues would be revealed by industry competitors, law enforcement or external security researchers.

A key point to highlight in these numbers is speed. Rapidly spotting and containing breaches is the primary mechanism for consistent and long-term resilience. Breaches are a given, but cybersecurity leaders are faster at detecting and responding. They can find and stop breaches before significant damage is done. They spot anomalies, trigger an investigation and eradicate the threat. Non-leaders, by contrast, over-spend on defense and under-spend on detection and response.

03

Choosing the right technologies

Increasingly sophisticated technologies are available in the cybersecurity area, and insurance cybersecurity leaders know which of them are best positioned to help reach a broader level of cybersecurity effectiveness. Our cyber resilience survey found that two technologies in particular are especially important to leaders:

Security Orchestration Automation and Response (SOAR)

Artificial Intelligence (AI): Machine learning, natural language processing

The use of these technologies helps to explain how cyber resilience leaders detect attacks faster and recover sooner. SOAR allows very rapid response to common incidents such as malware on a user's computer. These types of routine issues can overwhelm security teams, leaving them with no time to search for and respond to the real adversaries.

AI can take companies beyond today's cybersecurity emphasis that is primarily on detection and remediation. Such a reactive approach is generally less effective at combatting the volume and relentlessness of today's threats. AI and machine learning offer new possibilities. When combined with the cloud, AI can help scale cyber defense efforts through smart automation and continuous learning that drive self-healing systems—automatic correction of cloud security assets to meet security policies. The learning process also helps to spot vulnerabilities. Security professionals can then augment the machine learning and algorithm process with human checks and verifications that reduce the risk of false positives.

04

Do you want to be a cybersecurity leader?

04 DO YOU WANT TO BE A CYBERSECURITY LEADER?

That may appear at first to be an odd question (who doesn't want to be a leader?). However, some insurance firms might not be attracted to a cybersecurity leadership position because they associate it with being difficult and expensive. They might believe that they don't need to be as good as the very top echelon of firms, but rather just as good as the competitor up the street.

However, a better way to think of "leadership" in this area is companies that "lead the way." Leaders are pathfinders. They don't necessarily spend the most amount of money. (In fact, over a 10-year period, they might actually spend less.) Instead, they spend it wisely and efficiently, and in a balanced way. They invest equal amounts on automation technologies and on detection and response rather than all of it on perimeter defense—something that our cyber resilience survey respondents said they had overinvested in. So, it doesn't mean that leaders buy the most expensive technologies that keep out the most sophisticated adversaries. It means they have a detection capability that allows them to spot issues and eradicate them quickly. On that basis, we believe it is essential that you "follow the leaders," because any other path is ultimately cost-prohibitive and unsustainable.

Some insurance firms might not be attracted to a cybersecurity leadership position because they associate it with being difficult and expensive.

More specifically, cybersecurity leaders in insurance tend to:

Prioritize speed

According to our survey, leaders invest with an eye on improving operational speed. The top three measures of cybersecurity effectiveness named by leaders all emphasize speed: how quickly they can detect a security breach, how quickly they can respond, and how quickly they can get operations back to normal. Beyond these priorities, leaders also measure the effectiveness of their resiliency (how quickly they recover from a breach) and their precision (improving the accuracy of locating cyber incidents).

Scale more

The rate at which surveyed organizations scale investments across their business has a significant impact on their ability to defend against attacks. The leaders best at scaling technologies—defined as having moved 50 percent or more of their tools from pilot to full-scale deployment—perform four times better than the average respondents.

The ability to scale is an important factor in the reach of security programs. The cybersecurity programs for those that are best at scaling actively protect three-fourths of all key assets in the organization, according to our survey. Average performers cover only one-half of their key assets. It is little surprise that 86 percent of leaders agreed that new cybersecurity tools are increasing cybersecurity coverage for their organizations.

Train more

The speed with which organizations in our survey find security breaches is faster for those who provide higher levels of security-related training. Fifty-nine percent of top performers among our insurance respondents offer training about security tools to more than half of users, compared with just 29 percent of non-leaders. Across the global sample, those who were top performers in terms of training found 52 percent of security breaches in less than 24 hours, compared with only 32 percent for average performers. Time to remediate a security breach also appears to be improved through better training.

Collaborate more

The organizations best at collaborating—the ones using more than five methods to bring together their strategic vendors and collaborators, the security community, cybersecurity consortiums, and an internal task force to increase understanding of cybersecurity threats—are twice as successful as others at defending against attacks. Organizations that collaborate more have a breach ratio of 6 percent versus an average of 13 percent for the rest.

Cybersecurity challenges are daunting, to be sure. In fact, our survey found that 83 percent of insurance survey respondents say that their security investments are failing them. This situation won't be addressed with a single stroke. Rather, becoming more strategic with security investments is often incremental in nature. Know what's currently possible to control and what isn't, and prioritize investments to increase your sphere of control wherever possible.

05

Immediate actions and takeaways

Certainly, the biggest warning flag raised in this latest edition of the "State of Cyber Resilience" report from Accenture is the growing threats from indirect attacks—those made through vulnerabilities in the defenses of vendors, partners or subsidiaries.

The answer to this problem is fairly easy to explain, though much harder to implement and manage over the long term. It is to put in place the policies, governance and enforcement such that any third party connected to your network requires the same security standards that you do. Otherwise you've got to treat them completely at arm's length. If you do not follow this policy, your network is only as secure as the least secure entity connected to you, and all of your security spending might be going to waste.

When we turn to the issue of subsidiaries, we see the problem in stark relief. Companies may presume that they are treating those entities as a separate company, but in fact electronic trust is most likely fully established between them. Emails from subsidiaries, for example, are usually not marked "external." That means that a security compromise at the subsidiary gives an attacker a perfect platform to send phishing emails to the parent company. Soon, the parent's network is compromised, as well.

Given finite security resources, there is value in a data-driven, business-focused approach to securing the enterprise ecosystem. This may mean using threat intelligence reports to risk-prioritize which vendors are in need of better security solutions. A managed security services approach can help an organization keep vendors or subsidiaries at arms-length, where they are not connected to the parent company's' systems, including its security apparatus. This approach can help tackle issues at a larger scale and with a wider scope, without burdening the corporate security department. By collaborating more broadly with others with the common goal of securing the enterprise and its ecosystem, organizations can help themselves while also helping smaller vendors, allies and partners to beat cybercrime.

Meeting your cyber resilience challenges with Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we allow clients to innovate safely, build cyber resilience and grow with confidence.

Follow us on Twitter @AccentureSecure
or visit us at accenture.com/security

About the authors

Chris Thompson

Chris Thompson is a Senior Managing Director, based in New York. He leads the Accenture Financial Services Security and Resilience practice. The Security and Resilience practice helps clients manage cyber risk: the subversion of information risk controls for the agenda of the perpetrator. The practice unifies security, operational risk, fraud and financial crime and provides end-to-end services across strategy, simulated attacks, consulting and managed services delivery. Chris has nearly 30 years of experience with large-scale change programs, working with some of the world's leading retail, commercial and investment banks.

David Fitch

David Fitch is a Managing Director based in Los Angeles, and is the North American Insurance Lead with Accenture Security. Over the course of his industry (CISO) and consultancy career, David has led a number of large-scale transformation programs in the security space, and developed long-term strategies to meet regulatory and board requirements. David brings a pragmatic approach to advising clients, with a focus on meaningful risk reduction, and a detailed understanding of insurance business operations.

Andrea Agosti

Andrea Agosti is a Managing Director, European Financial Services Lead with Accenture Security. He has over 20 years of experience in the areas of IT risk, security strategy, cybersecurity, business resilience, financial crime and cyber regulations for financial services. In Andrea's current role he helps financial services organizations and their executives in Europe strengthen their security capabilities and functions and build a security lifecycle from the inside out to respond to current needs and future challenges.

Stay connected

Accenture Finance and Risk
www.accenture.com/us-en/services/financial-services/finance-risk

Finance and Risk Blog
financeandriskblog.accenture.com

Connect With Us
www.linkedin.com/showcase/16183502

Follow Us
www.twitter.com/AccentureFSRisk

About Accenture

Accenture is a leading global professional services company, providing a broad range of services in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched experience and specialized capabilities across more than 40 industries—powered by the world's largest network of Advanced Technology and Intelligent Operations centers. With 513,000 people serving clients in more than 120 countries, Accenture brings continuous innovation to help clients improve their performance and create lasting value across their enterprises. Visit us at **www.accenture.com**