HIGH PERFORMANCE SECURITY REPORT 2016

Accenture Security

INSURING YOUR FUTURE

CYBERSECURITY AND THE INSURANCE INDUSTRY

RESULTS FROM THE

ACCENTURE HIGH PERFORMANCE SECURITY REPORT 2016

How are insurance companies faring when it comes to protecting their assets and their customers from fraud, malware, cyber attacks and a host of other security breaches?

The question is important. Insurance companies hold a vast amount of data including personally identifiable information, personal health information, credit card and bank account data, and trade secrets (their own and sometimes their clients'). Insurers have a very distributed model for servicing, increasing the risk across the value chain. Aging legacy systems complicate matters even more.

The focus of most news stories about security breaches has been the banking sector, but the risk in the insurance industry is equal if not greater. The ability of cyber crooks to monetize stolen data, enabled by the dark web and crypto-currencies like Bitcoin, has changed the focus of many attackers. The actual money is heavily guarded, even in cyber space, but personal data is much easier to steal.

Accenture has conducted a wide-ranging survey into the state of cybersecurity, and the results are not comforting. The survey (see "About the Research" on page 12) found that cybersecurity overconfidence is distinctly prevalent. Large percentages of respondents from the insurance industry were confident that they are doing the right things in terms of cybersecurity, with 79 percent of large insurers' security executives surveyed expressing confidence in their cybersecurity strategies and 72 percent believing they have embedded effective cybersecurity into their cultures.

Why is this so alarming? Because the reality of what's actually happening within a typical insurance company is quite different. From both external and internal sources, insurers continue to be at high risk from an information security standpoint.

The survey revealed that insurers are suffering from an astounding number of security breaches. In addition to thousands to millions of random attacks each week, a typical insurance organization will face an average of 113 targeted breach attempts every year, a third of which will be successful. That's more than three effective attacks per month, pointing toward a serious dissonance between cybersecurity confidence and cybersecurity capability.

Figure 1. Insurers have confidence in their cyber capabilities. Are they being overconfident?

of insurers say that it takes months to detect successful security breaches

4 out of 5

insurers express confidence in their abilites to protect their organizations from cyber attacks.

113

targeted cyber attacks are directed at the average insurer every year.

72%

say they have completely embedded cybersecurity into their cultures.

1 in 3

targeted attacks result in a security breach. That's more than 3 effective attacks per month.

Source: Accenture High Performance Security Report 2016

DETECTION TAKES TOO LONG

Of course, breaches are only a problem if they are not detected. It is important to have defense in depth rather than simply a tough exterior. However, the length of time taken to detect these security breaches demonstrates that the attackers are spending considerable time inside the organizations. Sixty-one percent of insurance respondents admit it takes "months" to detect successful breaches. Additionally, internal security teams in the insurance industry discover only 66 percent of effective breaches. Who finds the rest? Usually employees, law enforcement or "red teams" (e.g., "ethical" hackers). Most survey respondents say that the company most frequently learned from employees about breaches not detected by the security team.

In fact, an insurer's people represent a very important part of its defense. In our experience, many attacks are successful because they exploit employees' login credentials—pointing to the importance of security training at every level of a firm and of continuously refreshing cyber talent across the business. Surprisingly, however, only 16 percent of insurers say they would invest in cybersecurity training.

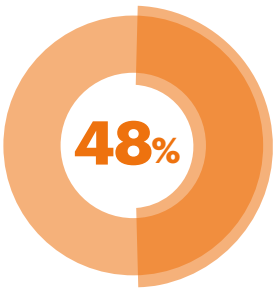
Clearly, insurers should ask themselves some in-depth questions about their cybersecurity approaches, where their risks are, and where they intend to invest. (See sidebar, "Asking tough questions about cybersecurity.")

FOCUSING
ON EXTERNAL AND INTERNAL THREATS

Prioritizing where to focus resources to adequately protect the organization from cyber attacks is a challenge for many insurers. Most firms continue to focus a majority of their resources on external security issues.

This external focus can potentially compromise the ability to address high-impact internal threats. Indeed, 48 percent of insurers say their greatest security threat comes from malicious insiders, but 55 percent also say they lack confidence in their organizations' abilities to monitor internally for breach activities—whether those are careless mistakes, failure to follow proper procedures or the result of malicious intent.

Insurers' internal security teams discover only 66% of effective breaches.



of insurers say the greatest security impact comes from malicious insiders

The widespread belief that you can trust your employees is a curious position for insurers to assume. After all, when it comes to claims disbursements, insurers have not traditionally been passive at all. Strong controls have always been in place.

Creating a strong culture of cybersecurity is critical—a culture extending from the newest hires all the way up to the C-suite. Training and communications have an important role to play, but culture change is really about changing behaviors. Employees and executives should use digital technologies with a full understanding of what security means to their job and everything that they do. Security is not just an IT problem. It's a company problem, and even a people problem.

TAKING A MORE HOLISTIC APPROACH

Most insurance organizations have a well-defined risk management process for core functions such as underwriting and investments. Insurers are, after all, in the business of risk transfer. Surprisingly, however, governance is a major challenge when it comes to cybersecurity because it extends across an organization's operations. Only 37 percent of insurers have a clear cybersecurity chain of command, and only 34 percent have proper cyber incident escalation paths.

Accountability and oversight are spread across C-level roles. Insurance organizations recognize that threats exist, but they often lack the holistic capabilities to proactively identify, understand and respond in an effective manner across multiple lines of defense.

ASKING TOUGH QUESTIONS ABOUT CYBERSECURITY

Insurers should answer several critical questions to reframe their cybersecurity perspectives and build a new definition of success:

- Are we confident that we have identified all priority business data assets and their locations? Are they segregated from less critical data?
- Are we able to defend the organization from a motivated adversary? Do we know what tools and tactics they might use?
- How could these attacks affect our business?
- Do we know what the adversary is really after?
- How often does our organization "practice" its plan to get better at responses?
- Do we have the right alignment, structure and team members to drive the behaviors needed to realize our cybersecurity objectives?

of insurers have proper cyber incident escalation paths

Chief information security officers (CISOs) have a vital role to play. However, if they are to have an impact they should step outside their comfort zones (e.g. compliance audits and cyber technology) and materially engage with enterprise leadership on a day-to-day basis. Doing so would require security executives to speak the language of the insurance business to make the case that the cybersecurity team represents a critical pillar in the battle to protect and extend company value.

To develop more holistic capabilities, Accenture recommends a two-pronged attack—focused on cybersecurity assessment on the one hand, and attack simulation on the other. Each of these activities on its own provides valuable insights into an insurer's security program. However, when they are coupled and performed in parallel, the assessment results are seen in the context of a successful attack. It becomes much easier to prioritize and to demonstrate to leadership where funding should be applied (see Figure 2).

Figure 2. Cybersecurity assessment and attack simulation

MATURITY ASSESSMENT	ATTACK SIMULATION	BENEFITS
Holistic assessments across key cyber functions with additional clarity on cybersecurity measures	Technical insights from the mind of a "real" hacker well beyond the scope of a risk assessment	**Insights Beyond Control Testing**
Control design review and testing to provide a view of current-state maturity	Tangible proof points of how the cyber controls are performing against external threat factors	**Tangible Proof Points**
Impact to the organization's operating model, including the core business strategy, with clarity on responsibilities and oversight across the three lines of defense	Tangible technical findings drive program buy-in and alignment across the organization – "actual vs. theoretical hack"	**Operating Model Alignment**
Re-baselined perspective on how to achieve the organization's desired maturity level and reduce risk	Detailed technical attack report with specifics on the organization's ability to detect and respond to adversaries	**Clear Path to Maturity**
Recommendations that allow the business to meet increased regulatory expectations	Threat vectors designed to test highest risk data such as Personally Identifiable Information (PIL), Protected Health Information (PHI) and Payment Card Information (PCI)	**Regulatory Compliance**
Results provide a platform for risk-based decision making around the existing security program	Explicit technical recommendations to help close existing gaps and build a more robust control environment	**Organizational Risk Reduction**

Source: Accenture High Performance Security Report 2016

MATURITY ASSESSMENTS

Many insurers are challenged with developing and improving risk management standards at the pace of new emerging cyber risks. Our survey found that only 38 percent of insurance organizations are competent in business-relevant threat monitoring. The issue for insurers is to build risk management capabilities across the horizontals of the company and to integrate the risk management function into the existing operational risk programs.

Insurers should conduct a realistic assessment of their capabilities to protect against high-impact threats, whether internal or external. They should also recalibrate risk appetite, thresholds and metrics to address the evolving cyber risk environment.

Part of the assessment is validation and alignment to industry security standards as a means to build a more robust control management framework and gain credibility with regulators. In addition, it is critical to identify, adopt and continually measure the enterprise against a cybersecurity framework that can be tailored to an insurer's business and mission objectives. This approach can increase enterprise resilience and asset integrity. The ability to look at risk from a strategic (cyber program assessment) point of view provides the ability to draw cause-and-effect relationships for increased confidence regarding risk mitigation priorities.

Traditional assessments have been audits that are based on checklists. Today, such an analysis needs to be a true risk assessment that identifies the controls needed to mitigate each risk. The controls should be managed against an agreed risk appetite with a set of metrics that measures the risks against the scale of the problem. For example, rather than measure unpatched systems, insurers should track the number of unpatched systems that contain sensitive information or that are publically exposed.

ATTACK SIMULATIONS

Pressure-testing company defenses can help leaders understand whether they can withstand a targeted, focused attack. Insurers can engage a "red team" in sparring matches with their cybersecurity people and systems to assess preparedness and response effectiveness. (See sidebar: "Balancing cyber threats against your risk appetite.")

Attack simulations should also look at internal threats. Many organizations fail to limit internal access to key information, monitor for unusual employee network activities or regularly review access. Adversaries know what they want, but they do not know where key assets live.

Cybersecurity professionals have the advantage of knowing which key assets they should protect, yet our survey found that only 33 percent of cybersecurity investments in the insurance industry protect key assets, and only 32 percent of insurers are able to identify high-value assets and business processes.

By prioritizing energy and investments around these assets, organizations can build a more effective cybersecurity foundation. Instead of attempting to anticipate a seemingly infinite variety of external breach possibilities, insurers can concentrate on the relatively fewer internal incursions that have the greatest impact.

Red-teaming is not for the faint hearted, however. A security sparring match is similar in effect to military live-fire training programs. The red team enters into the production environment and could accidently cause substantial damage. However, red-team members follow strict protocols and controls. They have significant investments in tools that emulate the latest techniques of the bad guys but which have been pre-tested to cause no damage. They follow a careful playbook and are the opposite of lone wolf hackers demonstrating how clever they are. An effective red team shows just enough to prove what they have done so that organizations can learn and improve.

BALANCING CYBER THREATS AGAINST YOUR RISK APPETITE

Accenture's experience has shown that a trained, well-equipped hacking team can break into the computer systems of almost any business they target.

The question, however, is what level of sophistication they needed to use and how that compared with the risk appetite of the institution.

Did they need to get physical access to the computing infrastructure?

Was it possible to find unpatched machines and enter through an exploit?

Did it need a sophisticated phishing attack, or was it a basic attack?

Was the level of cyber defense adequate to deter the typical adversaries of the institution?

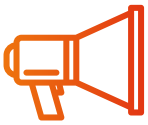
You can only answer these questions by understanding those adversaries and simulating the types of attacks they might make.

MAKING THE RIGHT INVESTMENTS

Insurers should innovate continuously to stay ahead of potential attackers, which may require redirecting some resources to new strategies and programs rather than investing more in current programs. (We found, for example, that 33 to 51 percent of insurers, if allocated extra budget, would spend it mostly on the same things they are investing in now.)

Organizations seeking to identify opportunities to invest in cybersecurity innovation should look in particular at seven key domains:

1. Business alignment assesses cybersecurity incident scenarios to better understand those that could materially affect the business.



2. Governance and leadership involves focusing on cybersecurity accountability, nurturing a security-minded culture, monitoring cybersecurity performance, developing incentives for employees and creating a cybersecurity chain of command.

3. Strategic threat context drives insurers to explore cybersecurity threats as a means of aligning the security program with the business strategy.

4. Cyber resilience is the company's ability to deliver operational excellence in the face of disruptive cyber adversaries. Our survey found that only 37 percent of insurers have systems and processes that are properly designed in accordance with cyber resilience requirements.

5. Cyber response readiness means having a robust response plan, strong cyber incident communications, tested plans for the protection and recovery of key assets, effective cyber incident escalation paths, and the ability to obtain solid stakeholder involvement across all business functions.

6. The extended ecosystem should be ready to cooperate during crisis management, develop third-party cybersecurity clauses and agreements, and focus on regulatory compliance. Our survey found that only 38 percent of insurers are competent at dealing with third-party cybersecurity, and only 36 percent are competent at cybersecurity regulatory compliance.

7. Investment efficiency strives to drive financial understanding concerning investments across cybersecurity domains and the allocation of funding and resources.

A focus on these domains can improve an insurer's cybersecurity capabilities and strengthen its resilience to cyber attacks. However, this can require continuous and systematic security investments. Looking across the entire financial services industry, only about a third of survey respondents expressed confidence in their capabilities in any of the seven cybersecurity domains, which highlights a need to make investing in these areas a priority.

The survey found that both overspending and underspending are common occurrences when it comes to cybersecurity. The good news: About four in ten financial services institutions spend between 7 percent and 10 percent of their IT budget on cybersecurity, a range we consider appropriate. The not-so-good news: 2 in 10 firms overspend, allocating over 11 percent of their IT budget; and 40 percent underspend, coming in the 4 percent to 6 percent range. Both point to an unbalanced cybersecurity risk management strategy.

CONCLUSION

BUILDING JUSTIFIABLE CONFIDENCE

Effective cybersecurity requires insurance organizations to gain greater maturity and improve their ability to protect the business from devastating losses. Challenges are coming from many directions, including regulatory pressures and increased customer expectations.

Fortunately, insurers have met these kinds of challenges and demands before. A case in point is the innovation driven in the industry by the low interest rate environment. Feeling the bottom-line impact of this threat, firms quickly began to act.

A similar reaction is beginning to happen now with cyber security. As their digital security strategies and organizations mature and new solutions emerge, insurers that tie cybersecurity efforts to real business needs can gain justifiable confidence in their ability to deal with cyber threats.

FOR MORE INFORMATION

Chris E. Thompson,
Senior Managing Director,
Accenture Security—
Financial Services North America
chris.e.thompson@accenture.com

Nadine Moore,
Managing Director,
Accenture Security—
Finance & Risk Services North America
nadine.moore@accenture.com

ABOUT THE RESEARCH

Accenture surveyed 183 security executives from the insurance sector via a hybrid online and telephone interview process. This constituted an important subset of the 2,000 executives surveyed as part of the global, cross-industry study. (To read the full report, follow this link)

The goal of the research was to understand how companies approach cybersecurity, how comprehensive their plans are, and where they prioritize spending.

The survey aimed to measure security capabilities across seven cybersecurity strategy domains identified by Accenture: business alignment, cyber response readiness, strategic threat intelligence, cyber resilience, investment efficiency, governance and leadership, and the extended ecosystem.

JOIN THE CONVERSATION


Read our blog


Linkedin


Twitter

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 373,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.