accentureconsulting

INSURING THE FUTURE

2018 State of Cyber Resilience for Insurance

OVER-CONFIDENCE?

Insurance companies have several things to be happy about in Accenture Security's comprehensive research study, 2018 State of Cyber Resilience.

For example, the percentage of successful security breaches has decreased from 30 percent of all attacks last year to 22 percent. The number of cybersecurity capabilities rated by Accenture Security as "high performing" among insurance respondents significantly increased—from 12 to 20 (out of 33; see Figure 1). High-performing capabilities included: "cooperation during crisis management"; and "peer monitoring – as a source for information on threats to your business."

Across all technologies and capabilities examined in the survey, about 80 percent or more of insurance executives are "confident" or "extremely confident" about their effectiveness. That might seem reasonable given the progress, but a case can be made that leadership is overconfident. Attackers are becoming increasingly sophisticated and attacks can shut down the business or expose customer data. If about one in five attempted breaches is successful, that's still a lot of breaches. And, given the findings that 45 percent of breaches are not detected for more than a week (9 percent require more than a month), that's a lot of risk exposure.

Financial services companies in general believe that their cybersecurity is tighter than that of other companies, but many industries have caught up. High-tech and consumer goods and services, for example, achieved "high performing" ratings for 19 capabilities. Life sciences had 21. Mastery of cyber resilience is key to reducing risk to a manageable level, and insurance is far from that level. Improvement has been steady, but it should still take two to three years for companies to reach a state of high-performance cyber resilience.

The number and sophistication of cyberattacks are increasing and are likely to get worse. Advanced technologies are likely to play important roles in the future of both cyberattacks and cyber resilience in insurance. But in the context of cyber defense, fewer than half of the companies surveyed are investing in advanced technologies such as artificial intelligence (AI) and machine learning (43 percent), or in automation technologies (39 percent). These are the types of technologies used by cyber criminals to perpetrate Distributed Denial of Service (DDOS) attacks at scale. If insurance companies don't keep up with the latest tools, then their cyber risk is expected to increase.

Figure 1: Assessing insurance cybersecurity capabilities

To assess cyber resilience in the insurance industry, Accenture Security evaluated 33 cybersecurity capabilities across seven domains

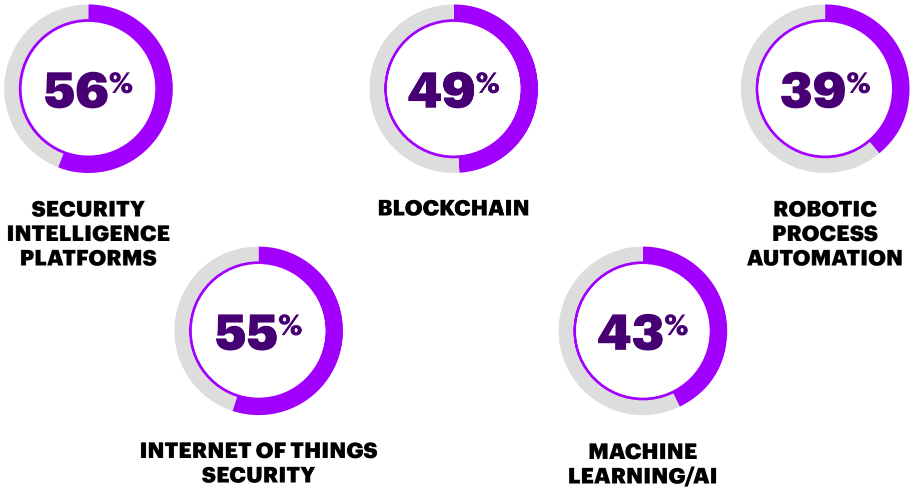
BUSINESS EXPOSURE	High-Value Assets and Business Processes	Physical and Safety Risks	Cyber Attack Scenarios	IT Risk Support	Cybersecurity Strategy
CYBER RESPONSE READINESS	Cyber Response Plans	Cyber Incident Escalation Plans	Cyber Incident Communication	Stakeholder Involvement	Recovery of Key Assets
STRATEGIC THREAT CONTEXT	What-If Analysis	Business-Relevant Threat Monitoring	Peer Situation Monitoring	Threat Vector Monitoring	
RESILIENCE READINESS	Recovery Ability	Design for Resilience	Exposure-Driven Design	Continuous Improvement	Threat Landscape Alignment
INVESTMENT EFFICIENCY	Securing Future Architecture	Security in Project Funding	Protection of Key Assets	Security in Investment Funding	Risk Analysis and Budgeting
GOVERNANCE & LEADERSHIP	High-Value Assets and Business Processes	Physical and Safety Risks	Actual IT Support	Scenarios of Material Impact	Key Protection Assumptions
EXTENDED ECOSYSTEM	Contractual Dependability	Operational Cooperation	Contractual Assurance	Regulatory Compliance Focus	

Source: Accenture, 2018 State of Cyber Resilience study

The cybersecurity situation facing the insurance industry is more complex than for most other sectors. In addition to protecting their own transactional and customer data, insurers are expected to increasingly offer policies to protect the digital assets of customers. In both cases, harnessing the power of advanced technologies is critical.

Figure 2: The use of advanced cybersecurity technologies in the insurance industry

In which of the following new and emerging technologies are you investing to evolve your security program?



Source: Accenture, 2018 State of Cyber Resilience study, insurance respondents

About the research

Now in its second year, Accenture Security's comprehensive research study, **2018 State of Cyber Resilience**, takes a closer look at the state of cyber resilience across key markets and geographies. Following interviews with 4,600 executives in 15 countries and across 19 industries, we discovered that the prospect of embedding cybersecurity into the fabric of the business is about two to three years away if current progress is maintained. There were 411 insurance industry executives surveyed as part of this study.

CURRENT CHALLENGES IN CYBER RESILIENCE

The cyber threat landscape is evolving faster than many companies are able to cope with, revealing critical security gaps.

Although many aspects of insurance are being rapidly digitized, many insurers are still operating legacy technology. Few have the luxury of moving everything to the cloud, leaving their "iron" behind. So most are digitizing on top of mainframes, and that makes for systems that are hard to protect from a cybersecurity perspective.

Data is another issue. Business decisions are increasingly data-driven, but the data environment is growing more complex as the volume of data multiplies. That data is made broadly available inside a corporation, sometimes across thousands of business applications. This availability significantly increases a company's risk profile.

The regulation situation is also unsettling. The European Union's General Data Protection Regulation (GDPR) has introduced stricter requirements for data protection, and similar regulation is being considered around the world. In the US, the New York State Department of Financial Services (NYDFS) has established 23 NYCRR Part 500, a mandatory regulation establishing cybersecurity requirements for financial services companies. The regulation requires covered entities to calibrate their cybersecurity programs by using periodic risk assessments to determine criteria to identify, evaluate and remediate risks by establishing appropriate controls and technological developments.[1]

Cyber threats are increasing in sophistication due to the availability of high-tech tools. The rise of the Internet of Things (IoT) means that the Internet itself may be weaponized with the proliferation of unsecured devices, and our offices and homes may be peppered with devices that can be used as hiding places and attack vectors for criminals. The Mirai botnet, a self-propagating botnet virus, used the IoT and automation to attack several types of companies.

In insurance, the industry is now seeing the intersection of fraud and cyber. In former days, fraud required the participation of other actors like doctors or auto body shops. Now, criminals just have to acquire the identity of a claims processer, or pretend to be an agent. Using stolen credentials, phishing attacks, social engineering or other cyber techniques can make that happen. Consequently, the growth of fraud has accelerated, can be committed faster and is lower risk for the criminals.

This is all happening at a time when cyber risks are expanding well beyond traditional enterprise boundaries to include alliances and business partners, vendors and others in a broader ecosystem. It also comes at a time when advanced security skills are in short supply.

[1] New York State Department of Financial Services 23 NYCRR 500 – Cybersecurity Requirements for Financial Services Companies," New York State Department of Financial Services. Access at: https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf

ACHIEVING MASTERY IN CYBERSECURITY

What would "mastery" in cybersecurity mean for the insurance industry? Although effectiveness across the 33 capabilities in our study is a stretch goal, here is a subset of capabilities that are particularly important for cybersecurity mastery.

Identify breaches quickly

To contain the damage caused by a cyber breach, companies should be able to recover within days if not hours. Yet for 67 percent of insurance companies surveyed, it requires more than 30 days to remediate a breach. Interruption of IT services is the most frequently cited result of a breach and causes the greatest loss.

Involve groups beyond the immediate cybersecurity team

Interestingly, the immediate cybersecurity team, by itself, identified only about two-thirds of all breaches (64 percent). Sixty-six percent of the remainder were identified internally by employees. Companies rely on their internal security workforce but supplement it with contractors and outsourced staff.

Focus on the right performance measures

The insurance companies in our study focus primarily on:

- **Cyber IT resiliency** (i.e., how many times an enterprise system went down and for how long)

- **Cyber recovery/restoration time** (i.e., how long it takes to restore normal business activity)

- **Cyber response time** (i.e., how long it takes to identify and mobilize)

Insurance companies in general struggle with metrics. They're in the business of risk management, of course. But their culture of risk management doesn't always reflect operational risk metrics; it's focused primarily on metrics related to underwriting losses. A culture change has to happen to think about risk in cyber terms.

Keep an eye on internal threats

The most frequent cyber threat identified in our study was an internal attack—i.e., caused by malicious insiders. The number of internal breaches experienced was even larger than for external hackers (see Figure 3). These risks are compounded because insurers have a large workforce of employees and contractors.

Extend cybersecurity standards across your ecosystem

Just 41 percent of insurance companies surveyed hold their ecosystem partners to the same cybersecurity standards as they do their own business (lagging the cross-industry findings by 5 percentage points). Insurers rely on claims ecosystems, which involve sharing data with a broad ecosystem and even with each other. So the risk of managing a massive number of connection points in the industry is high and growing higher.

Test and stress test

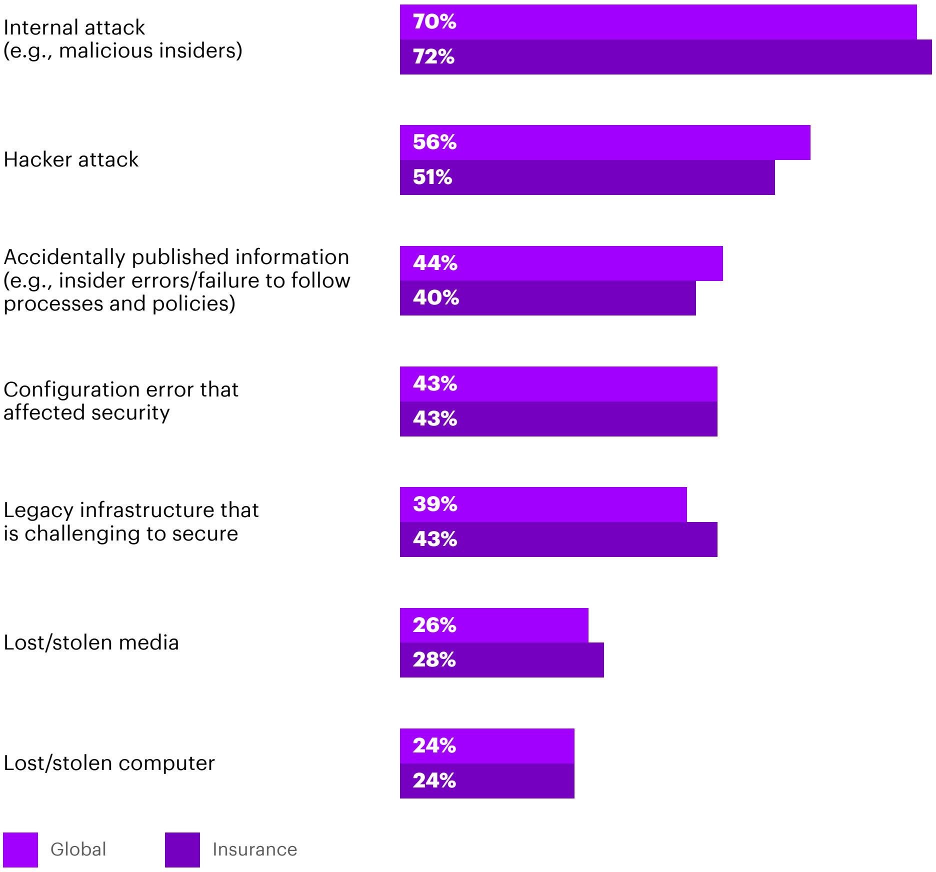
There is hardware involved with security, of course, but cybersecurity is primarily software. There is no substitute for testing it like you would any other software—particularly stress testing to identify vulnerabilities more rigorously than even the most highly motivated attacker.

Don’t overemphasize perimeter controls

Many companies have over-invested in advanced perimeter controls, probably in the hope that this can compensate for weaker security elsewhere. The problem is, criminals always seem to find a way through the perimeter, sometimes by manipulating insiders through **social engineering**. Think about the whole attack chain and make it as difficult as possible for the attacker at every step.

Figure 3: Most frequent sources of cybersecurity breaches

Among the types of breaches your organization has experienced, please rank them from most to least frequent. (Ranked top 3)



Source: Accenture, 2018 State of Cyber Resilience study, insurance respondents

THE FUTURE OF CYBER-SECURITY AND CYBER RESILIENCE

The rapid evolution of information technology will largely define the future of cybersecurity, from both an attack and a defense standpoint. It is important to look at the future of IT if we want to understand future security challenges. Three of the trends explored in the Accenture Technology Vision 2018 are particularly relevant to the future of cybersecurity at insurance companies and are discussed on the following pages.

1 Data veracity: The importance of trust

By transforming themselves to run on data, businesses have created a new kind of vulnerability: inaccurate, manipulated and biased data that leads to corrupted business insights and skewed decisions with a major impact on society. Cybersecurity teams are expected to be challenged more than ever to validate and protect data.

Furthermore, following an attack it is no longer sufficient just to execute the business continuity plan and restore the technology. Unless strict isolation protocols are applied and the exact start date of the breach is known, any recovered data is suspect. Procedures should be in place to reconcile and validate the data back to immutable systems of record, such as a blockchain of the original customer transactions. Few companies can do this today. Although the recovery timetables demanded by regulators or expected by customers are not as tight for insurance as they are for banking, recovery is still a major concern.

> **Cybersecurity teams will be challenged more than ever to validate and protect data.**

2

Frictionless business: Built to collaborate at scale

Businesses depend on technology-based relationships and alliances for growth, but their own legacy systems usually aren't designed to support collaboration with vendors and partners at scale. To fully power the connected intelligent enterprise, companies should first re-architect themselves. Each of these new offerings can only succeed with strong security as its backbone.

Insurance companies have always looked to take risks off other companies' books or to support individuals who suffer losses that would be catastrophic without coverage. As assets become digitized we have seen a spike in online theft. Insurance companies are encouraged to become "experts" in blockchain, security and cyber crime if they are to successfully insure this growing sector.

3

Internet of thinking: Intelligent distributed systems

As IoT devices become cheaper they are finding their way into everything from light switches and fire alarms to cars and industrial machinery. Insurance companies should be able to leverage telemetry from these devices to make better decisions around coverage and behaviors. But the decisions will only be good if the devices are secure and the data stream has integrity. New patterns of insurance fraud should likely emerge through data manipulation. New analytics and security controls would be needed to fight this.

CREATING A CYBER RESILIENT INSURANCE COMPANY

It is critical that insurance companies make sufficient investments and become much more sophisticated in the application of the breakthrough technologies that are increasingly being used by cyber criminals.

For example, automated orchestration capabilities enable security teams to respond in near-real-time, and advanced machine learning algorithms are replacing manual reviews to finally enable the cleanup of access management.

It is also important to pressure test your cyber resilience to mimic the actions of attackers. Enhance conventional red team attacks and blue team defense testing through things like coached incident simulation, threat intelligence and experienced player-coaches.

Finally, evolve the role of the Chief Information Security Officer (CISO) to be more integrated with the business. CISOs should be both business adept and tech-savvy. They should be equally at home in the C-suite and the security center, and approach the problem with a risk mindset. It is also vital to infuse a “security first” culture throughout the organization. The challenges are too great to be handled only by a central team. Everyone needs to be involved.

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 service delivery. Chris has over 20 years of experience in large-scale change programs, working with some of the world’s leading retail, commercial and investment banks.

NADINE MOORE

Nadine is a Managing Director with Accenture's Finance and Risk practice for the Midwest region, and is the cybersecurity lead for insurance. She is focused on delivering solutions for clients in the areas of cyber security, operational risk and controls, and finance transformation. Her insurance area of specialization is in property and casualty. She is also a licensed life and health professional and specialist in intangible risks.

STAY CONNECTED

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

Finance and Risk Blog
financeandriskblog.accenture.com

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

Follow Us
twitter.com/AccentureFSRisk

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 more than 449,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Its home page is www.accenture.com

DISCLAIMER

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.