HIGH PERFORMANCE SECURITY
REPORT 2016

BUILDING CONFIDENCE

SOLVING BANKING'S CYBERSECURITY CONUNDRUM

Accenture Security

RESULTS FROM THE ACCENTURE HIGH PERFORMANCE

SECURITY REPORT 2016

How are banks and other financial services institutions (FSIs) faring when it comes to protecting their assets and their customers from fraud, malware and a host of other security breaches? Accenture has conducted a wide-ranging survey into the state of cybersecurity, and the results are not comforting.

The survey (see "About the Research") found that overconfidence within the banking industry is alarmingly prevalent. Large percentages of banking respondents were confident that they are doing the right things in terms of cybersecurity, with 78 percent of large enterprise security executives surveyed expressing confidence in their cybersecurity strategies and 76 percent believing they have actually embedded effective cybersecurity into their cultures.

Figure 1. FSIs have confidence in their cyber capabilities ... are they being overconfident?

Compared to the global average, banks exhibit higher confidence in their cybersecurity capabilities because of:

...their abilities to:		...their top strategies are achieving desired business outcomes:	
1. Measure the impact of a breach:	**51%**	1. Protecting customer information:	**93%**
2. Identify the cause of a breach:	**51%**	2. Protecting company information:	**89%**
3. Manage financial risk due to a cybersecurity event:	**50%**	3. Preventing service disruption:	**78%**
4. Monitor for breaches:	**48%**	4. Protecting company reputation:	**76%**

78%

of companies agree that their organization is confident that their cybersecurity will demonstrate valuable results.

Source: Accenture High Performance Security Report 2016

In addition, high percentages of surveyed banking security and risk executives—higher than the global, cross-industry average from the research (see Figure 1) — believe their cybersecurity capabilities are achieving desired business outcomes, including:

- Protecting customer information (93 percent)
- Protecting company information (89 percent)
- Preventing service disruptions (78 percent)
- Protecting the company's reputation (76 percent)

The reality is very different, however, indicating a major disconnect or misalignment between the assumptions about security capabilities and what's actually happening in the trenches. From both external and internal sources, companies continue to be at high risk from an information security standpoint.

RECOGNIZING

THE THREAT

The survey revealed that financial services firms are suffering from an astounding number of security breaches. A typical financial services organization will face an average of 85 targeted breach attempts every year, a third of which will be successful.

That's between two and three effective attacks per month, pointing toward a serious dissonance between cybersecurity confidence and cybersecurity capability. In addition, 68 percent of firms surveyed agree that cyberattacks are "a bit of a black box." That is, firms don't always know what they don't know.

33% **OF ATTEMPTED BREACHES AGAINST FSIs ARE SUCCESSFUL[1]**

Of course breaches are only a problem if they are not detected. It's important to have defense in depth rather than simply a tough exterior. But the length of time taken to detect these security breaches demonstrates that the attackers are spending considerable time inside the organizations. Fifty-nine percent of banking respondents admit it takes "months" to detect successful breaches, while another 14 percent identify them "within a year" or longer.

Additionally, internal bank security teams discover only 64 percent of effective breaches. Who finds the rest? Usually employees, law enforcement or "white hats" (e.g., "ethical" hackers). Fully 99 percent of survey bank respondents say that the company most frequently learned about breaches not detected by the security team from employees. In fact, a company's people represent its best form of defense. In our view, 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.

DETECTING A BREACH TAKES MONTHS FOR

59%

OF FSIs SURVEYED[2]

Clearly, financial services firms 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 cyberattacks is a challenge for many companies. Most firms continue to focus a majority of their resources on external security issues. For example, 62 percent prioritize heightened capabilities in perimeter-based controls against outsiders.

This external focus can potentially compromise the ability to address high-impact internal threats. Indeed, 48 percent of surveyed banking respondents say internal breaches have the greatest cybersecurity impact, but 52 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.

48% **OF FSI RESPONDENTS SAY THE GREATEST SECURITY IMPACT COMES FROM MALICIOUS INSIDERS[3]**

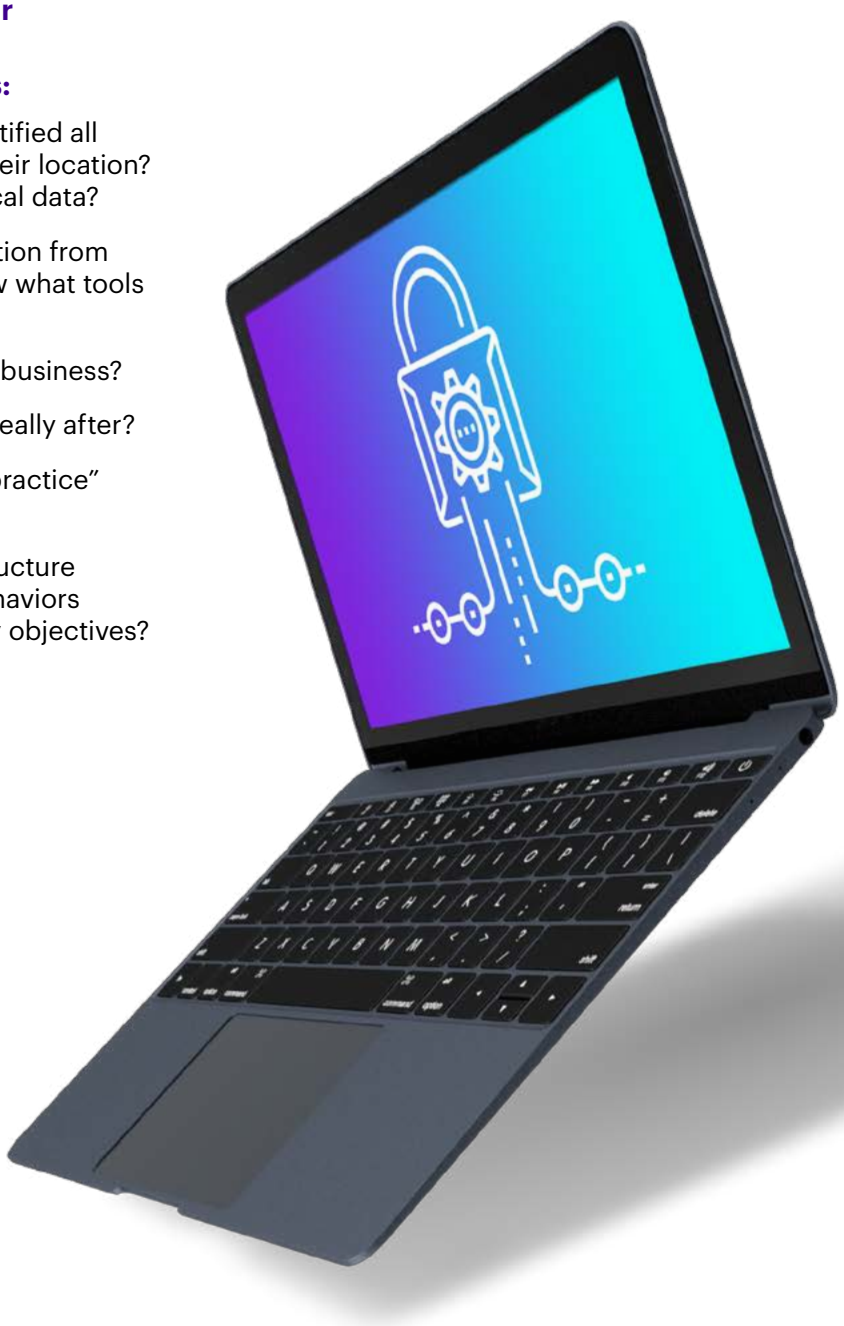
The widespread belief that you can "trust" your employees is a curious position for financial services companies to assume. After all, they have not traditionally taken that passive sort of view when it comes to customers' financial assets. Strong controls have always been in place.

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.

ASKING TOUGH QUESTIONS ABOUT CYBER SECURITY

Organizations 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 location? 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?



TAKING A MORE

HOLISTIC APPROACH

Governance is a major challenge when it comes to cybersecurity because it extends across an organization's operations. Thus, accountability and oversight are spread across C-level roles. Financial services organizations recognize that threats exist but often lack the holistic capabilities to proactively identify, understand and respond in an effective manner across multiple lines of defense.

Chief Information Security Officers (CISOs) have a vital role to play. But if they are to have an impact they should step outside their comfort zones (e.g., compliance audits, 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 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—one focused on cybersecurity assessment on the one hand, and attack simulation on the other. Each of these activities on their own provides valuable insights into an organization'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 performance 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 vectors.	**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 (PII), 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

Financial services institutions are challenged with developing and improving risk management standards at the pace of new emerging cyber risks. Organizations should conduct a realistic assessment of their capabilities to protect against high-impact threats, whether internal or external. They are also encouraged to 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, identifying, adopting and continually measuring the enterprise against a cybersecurity framework that can be tailored to an organization's business and mission objectives is critical to 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, 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. Organizations 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 don't know where key assets live. By contrast, cybersecurity professionals have the advantage of knowing which key assets should be protected. By prioritizing energy and investments around these key assets, organizations can build a more effective cybersecurity foundation. Instead of attempting to anticipate a seemingly infinite variety of external breach possibilities, organizations 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. 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 did that compare 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 they 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 your adversaries and simulating the types of attacks they might make.

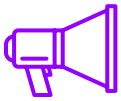
MAKING THE RIGHT

INVESTMENTS

Organizations 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.

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

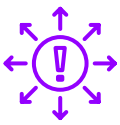
1. **Business alignment** assesses cybersecurity incident scenarios to better understand those that could materially affect the business.



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 organizations 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.



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.

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 a company's cybersecurity capabilities and strengthen its resilience to cyberattacks. However, this can require continuous and systematic security investments. Only about a third of total 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 banking 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 at the 4 percent to 6 percent range. Both these instances point to an unbalanced cybersecurity risk management strategy.

ON AVERAGE, BANKING INSTITUTIONS SPEND

8.2%

OF THEIR IT BUDGET ON CYBERSECURITY[4]

CONCLUSION

BUILDING JUSTIFIABLE CONFIDENCE

Effective cybersecurity requires financial services 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, financial services firms have met these kinds of challenges and demands before. A case in point is the huge push toward higher-quality banking services in the face of new competition. Feeling the bottom-line impact of this threat, firms quickly began to act.

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

Reference

1. Accenture High Performance Security Report 2016

2. Ibid

3. Ibid

4. Ibid

For more information

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

Floris van den Dool, Managing Director
Accenture Security—Financial Services, Europe, Africa and Latin America
floris.van.den.dool@accenture.com

Joseph Failla, Managing Director
Accenture Security—Financial Services, Asia Pacific
j.failla@accenture.com

David Pérez Lázaro, Managing Director
Accenture Security—Financial Services, Europe, Africa and Latin America
david.perez.lazaro@accenture.com

Stay connected

Accenture Finance and Risk
www.accenture.com/financeandrisk

Finance and Risk Blog
http://financeandriskblog.accenture.com/

Connect With Us
www.linkedin.com/groups?gid=3753715

Join Us
www.facebook.com/accenture

Follow Us
www.twitter.com/accenture

Watch Us
www.youtube.com/accenture

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 394,000 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.

About the Research

Accenture surveyed 275 security executives from the Banking 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 report. The report and additional support material are available here: www.accenture.com/BankingCyberSecurityReport. (To read the full report, follow this link: www.accenture.com/CyberSecurityReport)

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.

Disclaimer

17-1262