Technology

Rebuilding confidence in financial services through robust cyber security strategies

By Tim Elliott and Yemi Saka

accenture

High performance. Delivered.

• Consulting • Technology • Outsourcing

Rebuilding confidence in financial services through robust cyber security strategies

To reignite growth and rebuild customer trust, many financial services institutions are putting a greater emphasis on digital channels such as mobile banking. Success with these channels requires not just a user-friendly interface but also airtight security that customers can depend on.

With many transactions now conducted over the Internet, and many automated tools available to hackers, financial services companies are more vulnerable to cyber intruders. Given the recent conditions of the financial markets and the tarnished reputation of the financial services industry generally, security threats have become an executive management issue, not just a technical problem, as they affect operational continuity and can undermine the confidence of customers and business partners.

This paper offers six steps to guide financial services executives in mounting a proactive, high-performance approach to cyber security.

A complex equation

What portion of your customer base already interacts with your business online, and how fast are those segments growing? What new delivery channels are you considering for your financial services products? How will regulatory activity, acquisitions, or divestures affect your security strategy? How many of your teams are using a cloud-based application to share documents with a customer or vendor? Which of your software developers has recently used his credit card to provision a server on a cloud service? Are you certain of your ability to recover when a key data center suffers a cyber attack? Do you know which of your employees have run up a crushing load of debt or have another reason to turn rogue in your environment?

Banks, credit card companies, insurance firms, and other financial services institutions have invested heavily in information technology over the past decade to improve competitiveness and productivity. Most of these organizations have become highly dependent on the Internet for conducting transitions with their customers. The use of Internet services among customers and employees has become more pervasive through a myriad of wired and wireless devices used in the office, at home, in cars and cafes – often bypassing the standard corporate security controls and policy when connected to unsecure environments. Users are also requiring financial business applications to work seamlessly across multiple environments and devices including smart phones, tablet computers, and kiosks.

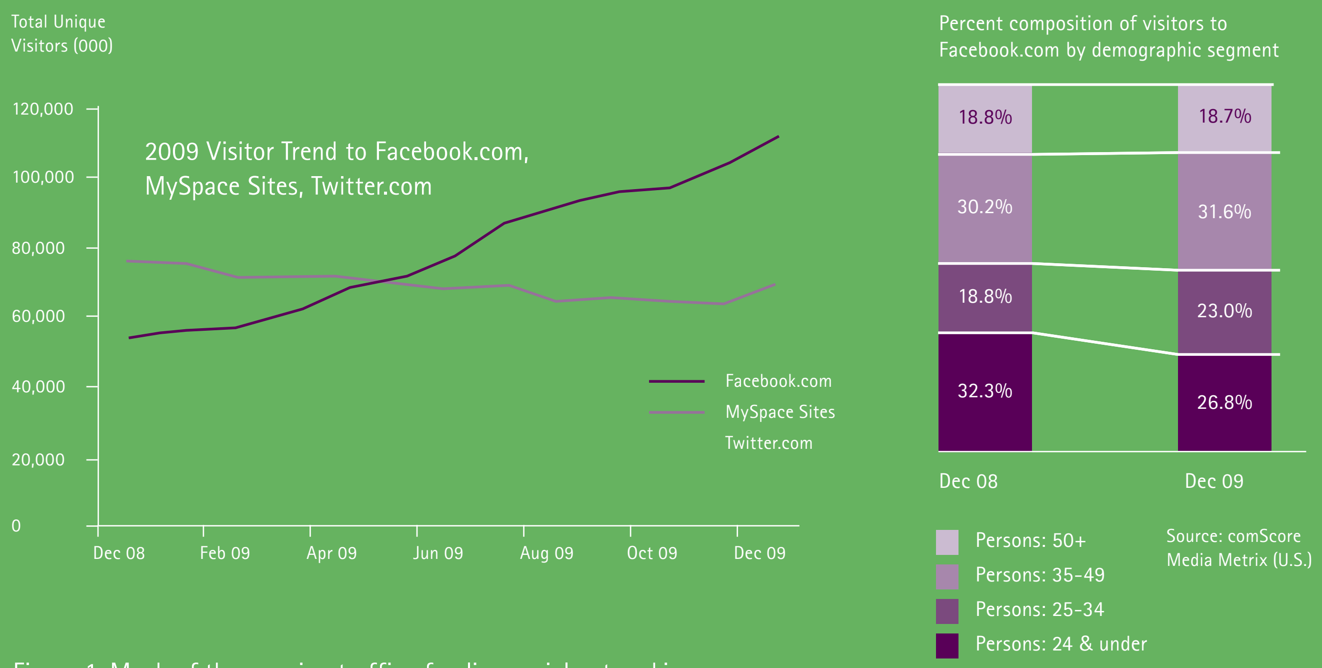
Customers want multiple access points and connectivity between them. In banking, for instance, customers show no desire to give up using branches, but at the same time they show increased usage of direct channels; the growth in use of mobile banking applications barely lags behind that of smart phone usage. In emerging economies, mobile banking has even leapfrogged traditional banking channels.

Tremendous benefits can accrue from open, distributed computing systems and the rich services offered by Google, Amazon, and others. And digital channels offer potentially greater personalization at radically lower cost – as long as customers trust the system's security. Accenture's 2009 Global Consumer Behavior Study asked customers to identify the dominant factors in their relationships with businesses. The top two factors cited were "easy to do business with" and "trustworthy".[1] That's the security challenge in a nutshell.

Unfortunately, the Internet has limitations on the level of security that it can provide when sharing information, and thus may become an easy target for malevolent use. Open systems, interfaces, and commonly used document formats can propagate vulnerabilities if appropriate security controls are not applied and enforced. Many IT solutions are built and released without the robust functionality now required for enterprise-wide data protection and privacy, particularly when projects focus on delivery speed rather than security.

Additional risks extend from incubating technologies, from the marriage of interoperable technologies that support cloud-based services, and from the new frontier of social media platforms (see sidebar, "Porous perimeters of social networking websites.")

Porous perimeters of social networking websites



Source: comScore Media Metrix (U.S.)

Figure 1. Much of the growing traffic of online social networking

Consider both the astonishing spread and the particular challenges of social networking sites. Nearly four out of five Internet users visited such a site in December 2009, and the activity now accounts for 11 percent of all time spent online in the United States, making it one of the most engaging activities across the Internet, according to comScore.[2]

Since the premise of social networking sites is to more easily and efficiently share personal information, site users tend to lower their guard. These sites thus become attractive locations for illegal data mining and malware insertion. One computer worm, Koobface, has targeted Microsoft Windows users of Facebook, MySpace, Friendster, Twitter, and similar sites to gather sensitive information such as credit card numbers. Although social networking companies have become more conscious of these threats, staying ahead of new attacks is a major challenge.

In another recent case, a hacker named Kirllos has been selling Facebook user names and passwords. Researchers at VeriSign estimate Kirllos has sold almost 700,000 of the 1.5 million accounts he or she is offering. The asking price: $25 to $45 per 1,000 accounts, depending on the number of contacts each user has.[3]

Other forms of malware tap users' "100 things about me" postings to mine data that is typically used to answer password-reset questions such as "What was your first pet's name?"

Once the security of an employee's laptop is breached through a social networking site, the company's systems and infrastructure become susceptible to cyber attacks. Yet blocking access to sites may not fully address the problem. For one thing, employees can often access the sites through their own smart phones – on which they may also check their corporate email. Moreover, many companies are themselves engaged in marketing and customer contact activities through these sites.

Another concern for financial institutions is how easily this type of information could be used to steal identities of employees and customers. Once an employee identity is compromised, intruders can take control of the employee's computer and slip inside the network, as occurred last year at one major financial firm.[4]

The most effective solution for the near term will consist of several elements: employee and customer education about safe online behavior; security controls such as Policy Enforcement Agents or Network Access Controls on the end user's device; and monitoring techniques that give an early alert on legitimate breaches versus mounds of false positives hiding these attacks.

Many of these applications deliver business benefits relatively quickly, but they often fall short of standard IT security policies and procedures. Even networked photocopiers or fax machines have their own Internet Protocol addresses that tend not be secured in the same way as a computer desktop, giving cyber attackers a path into the company. So the attack surface has gotten much broader, from many more sources at home and abroad.

With greater dependence on web-based applications comes a far more serious consequence of infrastructure compromises and disrupted operations through data breaches, data loss, and non-compliance with government regulations or important industry standards – along with the potential erosion of customer confidence.

In the United States alone, more than 346 million records containing sensitive personal information have been involved in security breaches since January 2005.[5] Such breaches can have serious implications for the enterprises involved, resulting in fines, increased costs for remediation, or temporary stock price drops. The threat is particularly acute for financial services firms, given that the storage and exchange of money forms the core of the business. A few heart-stopping data points:

- A May 2009 survey by Actimize found that 81 percent of financial services organizations expect an increase over the next year in ATM/debit card fraud.[6]
- Computer hackers stole more sensitive records in 2009 than in the previous four years combined, with ATM cards and PIN information growing in popularity, a Verizon study found. Organized criminal groups orchestrated nine in ten of the most successful attacks, with 93 percent of the records exposed coming from the financial sector.[7]
- Zeus and Clampi botnets, which steal online account credentials with a focus on bank accounts, have gained in size and strength in recent months. Cheap ($700), and easy-to-use toolkits that hackers can purchase to control botnets are widely available online.[8]

Customer information of all kinds is also at risk as online shopping and point-of-sale capture have become widespread, forcing various industries to adjust as a result. Every merchant that accepts credit card payments has already experienced the considerable cost and expense to strengthen protection against identity theft and the resulting financial losses.

The industrialization of cyber crime

Make no mistake; the adversaries have become smarter, better organized, and more persistent. Earlier this year, a crew of hackers was sentenced to prison for breaking into systems belonging to Heartland Payment Systems, a processor of credit card transactions. The crew sold millions of credit card numbers to Russian criminals and used some of the data to make unauthorized ATM withdrawals. Cyber criminals are also now targeting hotels to steal credit-card data from guests. The common weakness at hotels is the security surrounding point-of-sale software, which hotels use to process credit-card transactions.[9]

The proliferation of attacks and threats has pushed cyber risk management from primarily a technical problem to a high priority business problem meriting attention at the highest levels of the financial services organization. The increased breadth and depth of government regulation is forcing enterprises to invest more, to remediate legacy weaknesses, and to prepare for the minefields ahead.

Figure 2. Top 10 largest reported data breaches

Organization	Estimated number of people or accounts affected	Financial impact
Zurich Insurance	46,000 customer records	$3.6 million fine
Heartland Payment Systems	100 million transactions, 175,000 merchants	$41 million settlement
TJX Companies.	45 million customer records	$20 million in investigative costs
U.S. Dept of Veteran Affairs	76 million veterans' medical records	Not available
Card Systems -2005	40 million credit card accounts	Not available
U.S. Dept. of Veterans Affairs	17.5 million veterans	Laptop recovered, no financial impact
BoNY/Mellon	12.5 million	Not available
Certegy Check Services	8.5 million	$975,000 settlement
TD Ameritrade	6.3 million	Not available
CheckFree	Up to 5 million	Not available
Hannaford Bros.	4.2 million	Not available

Source: Privacy Rights Clearinghouse, reported at www.abcnews.com, June 14, 2010; Zurich fine: http://www.silicon.com/technology/security/2010/08/25/zurich-insurance-fined-2m-over-data-breach-39746267/

Core cyber principles for an uncertain world

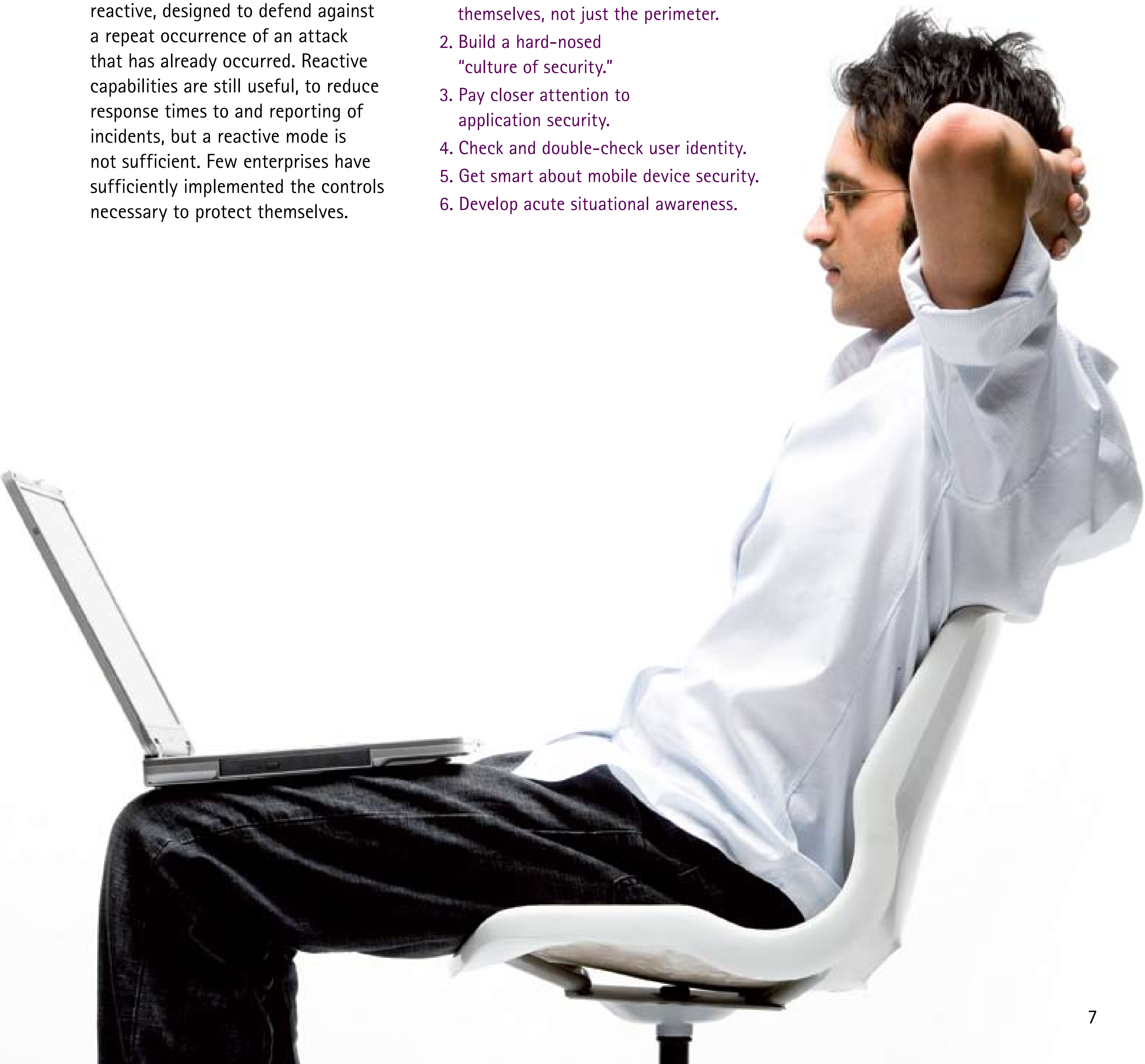
As senior executives weigh their next moves in cyber security, we advocate a proactive approach: Anticipate what new threats may challenge the enterprise and which security elements can help to improve performance; then weave the right security features into the enterprise's infrastructure and digital assets.

Getting ahead of the threats is not easy, to be sure. The measures taken in most financial services enterprises have been largely reactive, designed to defend against a repeat occurrence of an attack that has already occurred. Reactive capabilities are still useful, to reduce response times to and reporting of incidents, but a reactive mode is not sufficient. Few enterprises have sufficiently implemented the controls necessary to protect themselves.

Effective cyber security should be incorporated into processes throughout an enterprise, not just on the perimeter. As financial services firms build, acquire, or source the right combination of capabilities, the experiences of leading cyber security professionals offer up a set of six principles that have proven quite effective in guiding the development of a comprehensive cyber security strategy.

The key principles of cyber security

1. Identify and secure the IT assets themselves, not just the perimeter.
2. Build a hard-nosed "culture of security."
3. Pay closer attention to application security.
4. Check and double-check user identity.
5. Get smart about mobile device security.
6. Develop acute situational awareness.



The Key Principles of Cyber Security

1. Identify and secure the IT assets themselves, not just the perimeter.

Because of the complexity of their business model, many financial services firms don't know the channels through which all of their information assets are accessed or where they're specifically located (in vendor applications, mobile devices, partner networks, or elsewhere). Effective cyber security starts by knowing what data and technology are essential to serving one's customers, ensuring the information is protected, and making sure business continuity programs are clearly established. There should be a detailed plan to protect these assets and capabilities from being compromised, including a robust test of the plan to make sure that it's viable.

While organizations typically focus on securing the IT perimeter, that's no longer sufficient. It's more effective to secure the data or asset itself, wherever it travels and wherever it lives. Financial services firms should embed cyber resilience and defensive capabilities throughout the organization, not just individual components.

This is not always a straightforward task, as it requires navigating a maze of regulatory, compliance, privacy, and business demands. Current and pending compliance frameworks differ by country, by industry, and by activity within a company. An organization must be agile enough to keep pace with changes in demand and in the nature of cyber threats. Most initiatives thus will benefit from an end-to-end approach, from problem analysis to monitoring the controls that follow implementation of the solution.

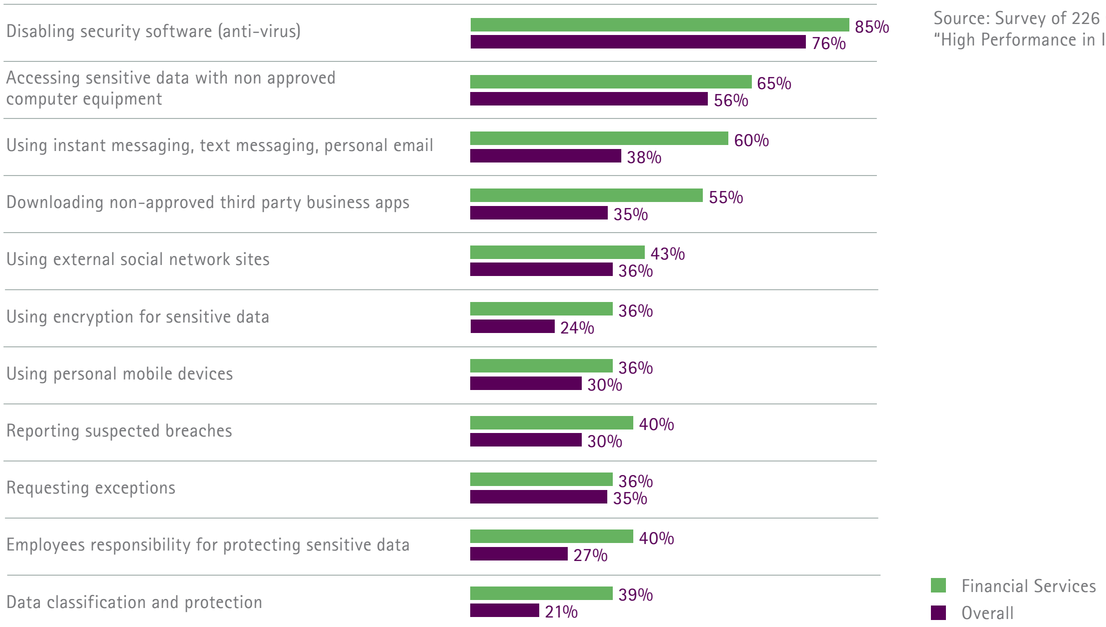
2. Build a hard-nosed "culture of security."

Financial services firms do not always clearly define cyber security governance structures, including specific oversight responsibilities. They may also find that the management responsibility and accountability can be dispersed and fragmented, with the Chief Information Officer, Chief Security Officer, Chief Privacy Officer, or the legal function all having some involvement. For instance, the CIO could be responsible for maintaining IT and data security, the CPO for setting policies and procedures, and the general counsel for ensuring the organization is complying with regulations. As a result, it's not clear where the buck stops on information security.

That's one reason for the big gaps in IT security policies among financial services institutions. As

Figure 3. Large holes in IT security policies

CIOs' response to "What portion of your organization do you believe is following your security policy related to:"



Source: Survey of 226 CIOs, part of Accenture's "High Performance in IT Research, 2010" shown in Figure 3, CIOs in financial services estimate that only about 40-60 percent of their workforce is following most policies, according to the new Accenture High Performance in IT Research, 2010.

By contrast, organizations that exhibit a culture of security do make responsibilities and accountabilities explicit. They go beyond the leadership levels and focus on employee awareness and accountability. Looking at examples from other industries, Sun Microsystems, General Electric, and Intel all have formally extended the remit of their privacy officer's role to information governance and/or data security to ensure a holistic approach to information management and protection.

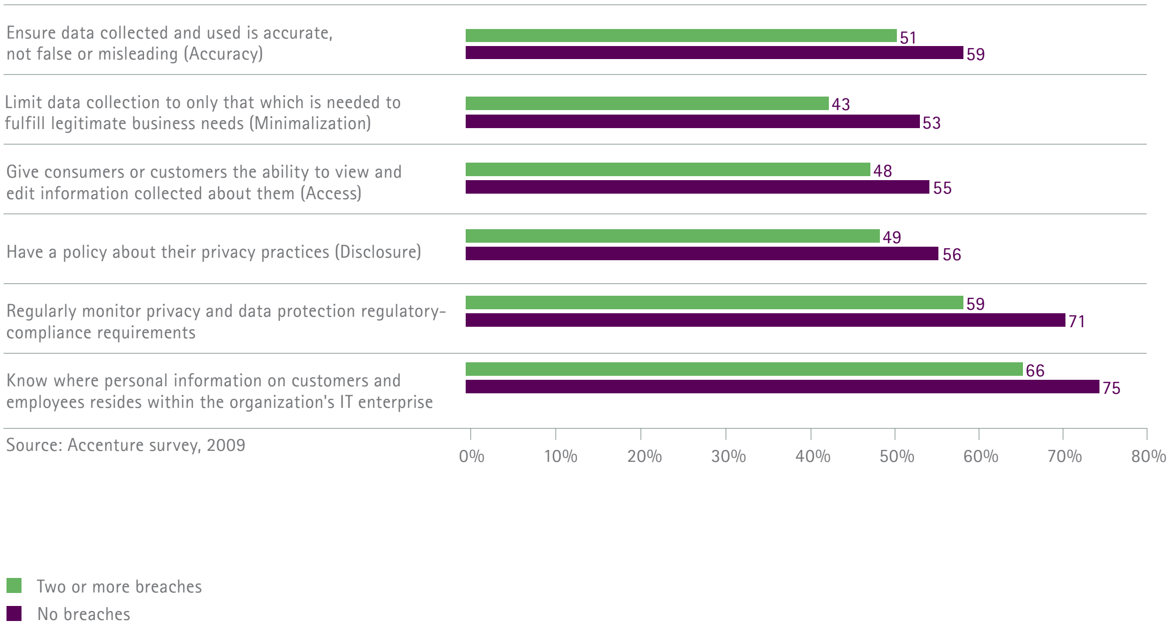
Some financial services organizations, such as Bank of America, have hired cyber security "czars" who have specific responsibility for cyber security strategy.[10] These executives lead such activities as the coordination of industry-wide exercises like the Cyber Attack against Payment Processes Exercise conducted recently by the Financial Services Information Sharing and Analysis Center.

Such organizations tend to view themselves as stewards, not owners, of personal data and take actions to protect data entrusted to them. Accenture's recent survey of business executives in 19 countries confirms that organizations with clear responsibilities and strong policies are less likely to experience security breaches, as shown in Figure 4.

The first step to building this culture is to put in place an IT governance program that integrates the people, processes, and technology needed to manage data effectively and efficiently. Effective governance programs typically start by defining roles and responsibilities for data owners and stewards. In some cases, it may make sense to establish a privacy and protection council, composed of stakeholders from across the business, which is responsible for overseeing how sensitive data is managed and used, as well as for continuous improvements of the organization's security posture.

Any data protection framework should address protection in a unified manner and avoid addressing regulatory compliance in separate silos of country, business process, or type of data. Organizations should create a common set of data privacy and protection standards that can be applied consistently from country to country to minimize complexity, cost of compliance, and chances for breaches while at the same time enabling responsible data sharing and global data flows.

Figure 4. Data protection policies matter
(percent of business executives responding)



Source: Accenture survey, 2009

3. Pay closer attention to applications.

Many serious breaches result from application-level weaknesses. Most applications were not engineered with security in mind, because developers assumed they would sit behind a secure perimeter. As that assumption is no longer valid, legacy applications will eventually have to be reengineered, and new applications need to be developed under a new security paradigm.

Nor is protecting the perimeter around applications enough of a defense, because firewalls or anti-virus solutions may not be comprehensive enough. Most financial institutions should extend security to the device level as well to the application layer.

Trusted applications development and delivery thus is a critical component of a cyber security initiative. Financial services firms need to be able to measure an application's resistance to attack and its ability to process and handle sensitive information regardless of who builds or maintains it. The system should undergo stringent testing to help confirm that mission-critical applications can be run with reduced risk.

There are two key issues here. First, designing consistently defined security services into applications as part of the system development lifecycle is a significant evolutionary step for an organization. The second, to test and remediate the existing applications to the same standard – whether they were built in house or purchased and installed or deployed at a vendor location – is another critical step in ensuring secure applications and the data they contain.

4. Check and double-check user identity.

Identity management has become a top security priority with the convergence of several trend: sharp increases in identity theft; risks associated with having an extended enterprise of customers, suppliers, and contractors with access to enterprise applications; and greater use of mobile devices that adds another interface to secure.

For many digital systems, the traditional paradigm of identity authentication is based on knowing phrases or numbers that once were considered secret or at least protected – such as one's Social Security number or mother's maiden name. Now much of that information may be commonly available or at least discoverable, undermining the premise of conventional authentication.

Mastering the ability to determine whether customers, suppliers or employees are who they claim to be when they access enterprise systems and facilities is crucial to enterprise performance. Yet with IT budgets under increased scrutiny, many CIOs are

Many serious breaches result from application-level weaknesses. Most applications were not engineered with security in mind, because developers assumed they would sit behind a secure perimeter.

charged with reducing risks and threats while also improving the administrative and cost efficiency of managing user identities and access to information.

Effective identity and access management programs should create value by embedding pervasive security without sacrificing functionality and ease of use. Aspects such as single-sign on, immediate access revocation when needed, self-service functionality, and real-time analysis to support audits are key components that will both support the business needs while also managing risk appropriately. Open-source protocols such as OpenID, which allow users to log on to different services with the same digital identity, are starting to catch on as a means of creating strong authentication combined with ease of use.

Financial services firms can take advantage of improving price-performance characteristics of other authentication technologies, such as biometrics (fingerprint or retinal scans) and smart cards, to speed the time to value and increase the return on investment of identity management initiatives. These trends are putting cutting-edge solutions in reach, even for organizations operating under fiscal constraints. Non-biometric, two-factor authentication is also useful for managing access and is more appropriate for some environments.

By combining stronger identity management methods with biometric technologies, companies can redefine how they do business. Larger retailers are already using "pay by touch" systems to verify the identity of customers who cash checks for payment of items. This helps simplify the check authorization process and reduce fraud.

5. Get smart about mobile device security.

Overall, mobile banking is expected to reach 400 million people in the next three years.[11] It has already become commonplace in Japan, many parts of Europe, and in some developing countries that leapfrogged older communications technologies to support their nascent micropayment systems. Whether through SMS-based payments, direct mobile billing, mobile web payments, or stored value cards, the technologies are starting to take hold in the United States as well. Other financial institutions are looking to mobile devices and are proliferating applications to take advantage of this channel.

For example, JPMorgan Chase & Co. is offering a mobile remote capture application that customers can use to electronically deposit checks with their phones. USAA Federal Savings Bank, which serves members of the military and their families, introduced a similar service last year.[12]

Many of the underlying technologies are similar to standard Internet banking. But for U.S. financial services institutions, several considerations come into play. First, there are new devices and new operating systems to consider – iPhone, Android, Windows mobile, BlackBerry, and others. Each of these has its own way of addressing security, which has implications to the development teams that need to compensate for security flaws across multiple services.

A related consideration is that mobile devices are easily lost or stolen. Most come with removable media such as a SIM card that may store a huge amount of personal data including account numbers and passwords, and can be breached relatively easily by a talented hacker. While consumers will turn first to their wireless telecommunications carriers for help with a stolen device, banks and other financial services firms cannot afford to sit on the sidelines.

A third issue is that many U.S. consumers have not yet grown accustomed to mobile financial services. Despite the spread of online banking and shopping through personal computers, consumers may not completely trust in the security of mobile payments when it's introduced. Unless consumers believe the system is safe and their personal data is secure, banks may face resistance to adoption of the new technology, or at least less cooperation by consumers in exploiting its potential.

Financial institutions should be preparing now for a sustained effort in consumer education and communications about mobile device security – good password protocol, how to erase data remotely if a device is stolen, and so on. The situation is similar to what banks had to do when they first introduced ATMs and more broadly when the Internet took hold. It may make sense to coordinate with telecom carriers in this regard, but banks should not wait for the telecom industry to take the lead.

6. Develop acute situational awareness.

Keeping ahead of risks means, first of all, understanding exactly which key risks the organization is facing – across the whole risk landscape, including employees and the business partner network, not just compliance status. Be aware of a risk's potential impact on the organization's overall performance, have a clear view of which risks might emerge, and have appropriate measurements in place to manage or mitigate these risks.

Addressing security in business network is a sensitive and complicated challenge because of all the players involved, but requires the same diligence as dealing with the internal organization. Organizations should collaborate with business partners that take equal or greater care with data, and rigorously assess

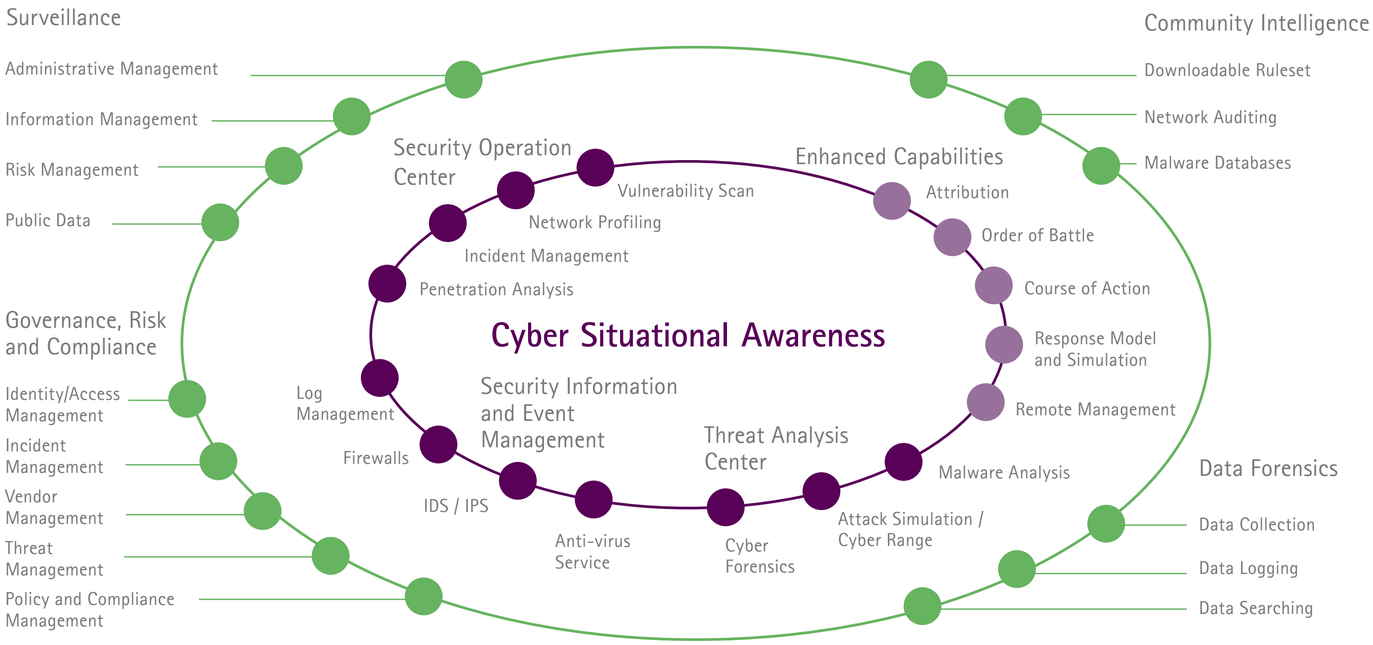


Figure 5. A situational awareness capability map

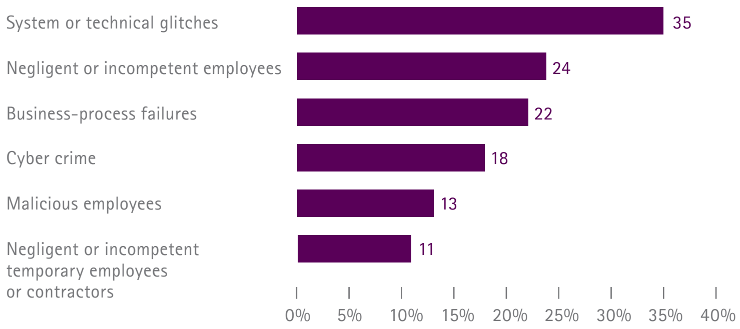
partners' knowledge, practices, and experience in managing sensitive data across organizational and national boundaries in accordance with local privacy laws and industry regulations.

Hackers and malicious entities search for vulnerabilities. For example, the day a merger of two financial institutions is announced, a wave of phishing emails typically go out to the merging banks' customers. The goal is to use this trigger event to gather personal information from one institution in the name of the acquirer, and thereby gain access to accounts. Another tactic is to exploit misaligned or lax processes and protocols between, say, a retail call center and the web channel for another line of business. After all, customer service agents want to help a caller and are paid to get them off the phone quickly, so they may be prone to giving valuable information away to a cyber attacker.

Banks and other financial services institutions therefore need to get more serious about monitoring suspect activity. It does no good to run a Security Information and Event Management (SIEM) system that generates 60,000 log line items every day if the log file is ignored and dumped at the end of the day. Security will fall short if a bank emphasizes cross-selling yet cannot correlate SIEM data across various lines of business. Moreover, if financial services organizations only react to suspicious activity, a recorded incident, onset of an attack, or a malware outbreak, it may be too late. They must also actively gather cyber intelligence and watch downstream activities in order to:

- Recognize back doors and vulnerabilities unseen by point compliance and checklist efforts
- Recognize complex and chained patterns that indicate the initiation of an attack
- Expand the scope of vulnerability assessment or penetration tests
- Harness external sources of threat intelligence to understand and train for zero-day exploits
- Detect reconnaissance activity by a terminated employee or a hacker forum

Application vulnerability scanner results, firewall rules, SIEM reports, chatter on blogs and forums as well as software vulnerabilities are readily available sources of threat intelligence. Layering and fusing these multiple sources of information helps to form an operating picture where the sum is greater than its parts (Figure 5).



Source: Accenture survey, 2009

Figure 6 Internal issues are frequent causes of security breaches
(percent of business executives responding)

Staying current with evolving threats will entail keeping staff educated and trained in cyber security. In a recent Accenture survey of business leaders and individuals, internal issues – employees (48 percent) and business or system failure (57 percent) were cited most often as the source of the breaches (Figure 6).

Beyond negligent employee behavior, insider fraud plagues financial institutions perhaps more than other industries. The problem could be an angry employee, or one overwhelmed by debt, who sells information about call center protocol to organized criminals. Or it might be a contractor dismissed for poor performance who programs a logic bomb before he leaves.

Pattern analysis tools, similar to customer relationship management tools, can help to flag anomalies in employee behavior as it occurs. Some financial institutions are also trying to be more predictive about insider fraud. They might require periodic urine testing, pull employee credit ratings frequently, or use similar techniques to anticipate which employees might turn rogue. Such activities may be opposed by some executives on grounds that they demonstrate a lack of trust, but most employees will accept these measures if the "trust, but verify" approach is communicated effectively.

Calibrating risk with cost when funds are tight

With each advance in technology that enhances connectivity and communication, the traditional corporate perimeter, with clearly identifiable boundaries, diminishes. In its place, a network with limitless potential is rising—one where financial institutions, their customers, and their partners demand access to information whenever and wherever they need it. Customers and partners will increasingly consider how the custodian of their data is going to protect sensitive information before embarking on a long-term relationship.

As a result, high-performing financial services players will take a more proactive and holistic approach to cyber security. Since attacks can be multipronged—via email, the web, and the network—the ability to view traffic across protocols and networks can improve an organization's ability to detect and block these attacks.

Cost and risk are the trade-offs in any security agenda. Some elements of a cyber security solution can be expensive, with the ROI difficult to quantify. It's not fun and it rarely adds to the bottom line – but the risk of a serious, highly publicized breach is equally hard to quantify and potentially catastrophic. As the pace of technology accelerates, an enterprise will have to calibrate its tolerance for risk in accordance with business requirements.

We also urge more pan-industry collaboration on cyber security issues, through groups such as the Financial Services Roundtable. An attack on one institution should be quickly communicated to others, so that they can better prepare. Even direct competitors can benefit from building a security community, without revealing their secrets.

Financial services leaders must take bold steps to ensure that security approaches and solutions are agile enough to adapt to rapid technological change today, while forging the right risk management program to support business growth and high performance.

Questions for executives

- Does each manager know what his or her responsibilities are with regard to information security?
- Do we assign ownership of and accountability for information security through a data governance program?
- Does our information strategy allow us to identify, track, and control how data flows across all our systems and processes?
- Have we evaluated our privacy and protection technologies to confirm they are providing the necessary level of protection?
- Have we built a consistent level of awareness among employees?
- Have we provided them with the appropriate guidance and training for how to handle sensitive data and create secure passwords?
- Are we proactive about spotting patterns that can signal internal fraud?
- Are we choosing business partners with care regarding their own security posture?
- Do we have a security strategy for mobile payments and mobile banking?
- Are we coordinating that strategy with the major wireless telecom carriers?

How Accenture can help

We address clients' information security priorities along the full spectrum of activities from strategy to implementation to operations. We understand the importance of working side by side with clients to build the requisite security capabilities in their own organizations. However we can also partner with clients over extended periods to run key security processes on an outsourced basis.

The challenges we address

There is a pressing need to transform the security and risk functions and move beyond pure compliance to value creation. We help financial services clients make better decisions and align risk and reward in the pursuit of business advantage on several fronts:

- Enhancing security capabilities and embedding a culture of security and risk management throughout the organization
- Proactively positioning the enterprise for potential stress situations and reacting quickly to fast-moving events
- Increasing cost efficiency despite mounting cyber threats and regulatory burdens such as Sarbanes-Oxley, the Patriot Act, and the Dodd-Frank Act
- Integrating technology solutions for transaction profiling across all types of fraud, including improved money laundering monitoring capabilities.

Best-of-breed information security solutions

Accenture offers a full spectrum of security capabilities including these core solutions:

- Identity and Access Management Services
- Application and Infrastructure Security Services
- Information Protection Services
- Security as a managed service

Notes

1 "Customer 2012: Time for a new contract between banks and their customers?" Accenture, 2010

2 "The 2009 U.S. Digital Year in Review," comScore, February 2010

3 http://www.networkworld.com/news/2010/042310-15-million-stolen-facebook-ids.html

4 "How cybercriminals invade social networks, companies," Byron Acohido, USA Today, March 4, 2010

5 http://www.privacyrights.org/ar/ChronDataBreaches.htm

6 http://www.actimize.com/index.aspx?page=news196

7 http://www.verizonbusiness.com/about/news/displaynews.xml?newsid=25282&mode=vzlong

8 "Annual Security Report," Cisco, 2009

9 "Data Breaches Are Heaviest at Hotels," The Wall Street Journal, March 18, 2010

10 "BofA Hires Data Security Czar," Penny Crosman, Bank Systems & Technology, May 20, 2010

11 "Mobile Banking to Reach 400 Million Users," Penny Crosman, Bank Systems & Technology, June 22, 2010

12 "JPMorgan Chase Now Offering Mobile Remote Capture App," Will Hernandez, American Banker, July 8, 2010

About Accenture

For more information on using security to achieve high performance in financial institutions please contact

Tim Elliott
t.elliott@accenture.com
+1-313-887-2636

Yemi Saka
Yemi.b.saka@accenture.com
+1 678-657-4735