Technology

6 Steps to Improve Cybersecurity

The Financial Institution's Guide to Securing Information – and Trust

accenture

High performance. Delivered.

In collaboration with

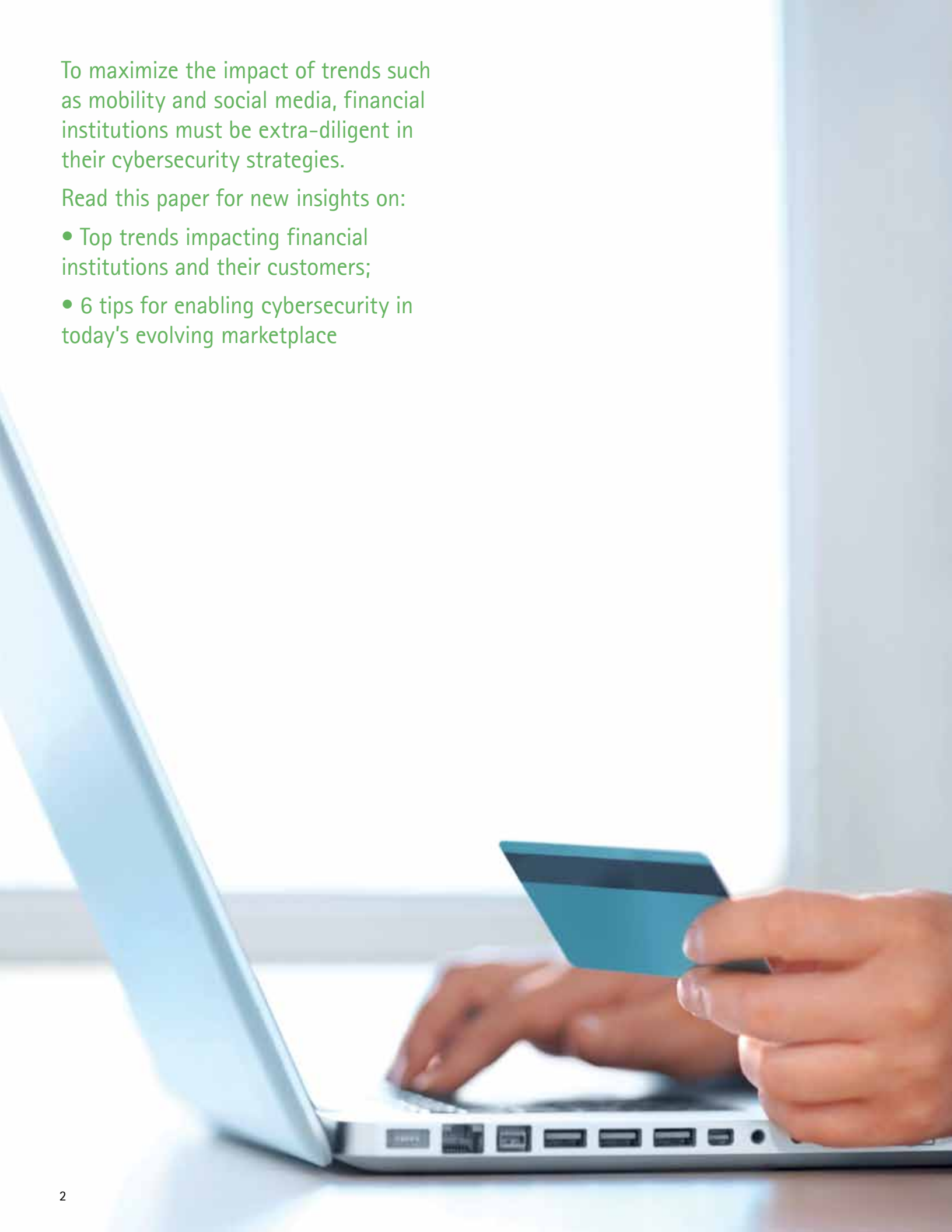
ISMG INFORMATION SECURITY MEDIA GROUP

• Consulting • Technology • Outsourcing

To maximize the impact of trends such as mobility and social media, financial institutions must be extra-diligent in their cybersecurity strategies.

Read this paper for new insights on:

- Top trends impacting financial institutions and their customers;
- 6 tips for enabling cybersecurity in today's evolving marketplace



Executive Summary

From making payments online to depositing checks via iPhones and communicating through Facebook, financial institutions in recent years have introduced many new services to make their customers' lives easier.

At the same time, institutions are empowering employees and partners with mobile platforms that rival traditional desktops; virtualizing infrastructure and moving services into the cloud. Such innovations bring real value to their customers, all the while affording institutions great efficiencies and cost savings.

But those same advances also put institutions at risk. And when the business is built on trust—as it is in any financial services firm—risk is not to be taken lightly.

"Trust is essential in financial services, as you're handling a very important portion of your customers' lives," says Greg Rattray, the new head of security for BITS, a division of The Financial Services Roundtable. "There are many factors today that could increase risk if you aren't doing the right things."

Still, he says, consumers continue to trust individual institutions. "This trust is what drives choice, in part, and enables banks to take advantage of new service opportunities."

New World, New Risks

Consumers look at their financial services partners in a whole new light. After all, much has happened in recent years—changes that have ultimately impacted trust and confidence levels. Perhaps the most damaging of late was the near collapse of the financial system in 2008. As a result, 171 U.S. banks and credit unions failed in 2009, and 181 failed in 2010.

Although the economy is on the rebound, uncertainty prevails, and institutions must do everything in their power to maintain consumer confidence. Cyber security is definitely an area that requires attention.

According to BankInfoSecurity.com, there were 62 reported breaches within financial institutions in 2009—nothing proved more notorious than the Heartland Payment Systems data breach, which affected 130,000,000 consumer accounts. In 2010, there were 58 breaches heading into December.

Also, according to the new "Faces of Fraud" survey from BankInfoSecurity.com, financial institutions consistently face a series of multi-channel threats, including the most popular forms of fraud: Payment card, check, phishing/vishing and ACH/wire.

The masterminds behind these attacks are persistent, patient and very sophisticated. They attack from every angle—from the traditional check and payment card fraud to new incidents of credit/debit card thefts via POS skimming, corporate account takeovers by way of ACH and wire fraud, unauthorized insider access within enterprise datacenters, or laptops stolen from mobile employees. Organized crime and terrorist groups take their cut, as well, with large-scale, targeted attacks using complex combinations of malicious code and exploits across multiple banking channels.

New Services, New Vulnerabilities

"Banks face a double challenge in that customers expect their money—and their personally identifiable information—to be kept secure," says Michael Seese, an information professional for a major midwestern bank, as well as author of the book Scrappy Information Security. "But they also want to be able to access their accounts at anytime from anywhere."

Financial institutions have responded to consumer demand with new service options that can prove dangerous. Among these new options:

• **Social Networking.** Social networking sites are commonplace today; an opportunity for institutions to reach key audiences. "But there are so many ways that social media can hurt a company," warns Seese. For example, an innocuous statement from an over-zealous employee—like, "Busy weekend coming up. I'll be working on the latest release!"—could be used by a competitor or a criminal. And many of the applications and games that are available on social media sites were crafted specifically to introduce malware to a user's PC.

• **Mobility.** Mobility has become paramount to sales, marketing and customer service strategies, as younger clientele especially clamor to conduct their banking business on the run from their mobile phones and handheld devices. That means institutions are creating services to do exactly that—from deposits to bill payments. Unfortunately, that new-found freedom introduces complexities, including a higher level of risk in terms of theft, malware and even direct attacks. And a lot of the risk is out of the institution's control and in the hands of customers with varying degrees of security savvy.

• **IT Consumerization.** Financial institutions empower employees with more business tools—smartphones, netbooks and laptops—that take data beyond the traditional perimeter. "I think most banks are doing it right, by providing them with corporate laptops and secure access methods, says Seese. But there have been mishaps that put consumers at risk. For example, TD Bank, N.A. and T.D. Wealth Management Services recently reported that a laptop containing customer account information was stolen from the office of the Securities and Exchange Commission in 2009.

• **Cloud Computing.** The cloud is the future for financial services, as in every other industry sector. The new delivery model promises cost savings and efficiencies as well as agility and innovation. But do institutions have sound strategies for putting sensitive data "out there?" asks Seese. As the custodians of confidential customer information, they are responsible for its safekeeping. So putting that data in the hands of a third party ups the ante in regard to security and compliance implications. Institutions can't afford to stick with old delivery models, but they have to approach the cloud with renewed focus on risk mitigation.

Risk Management

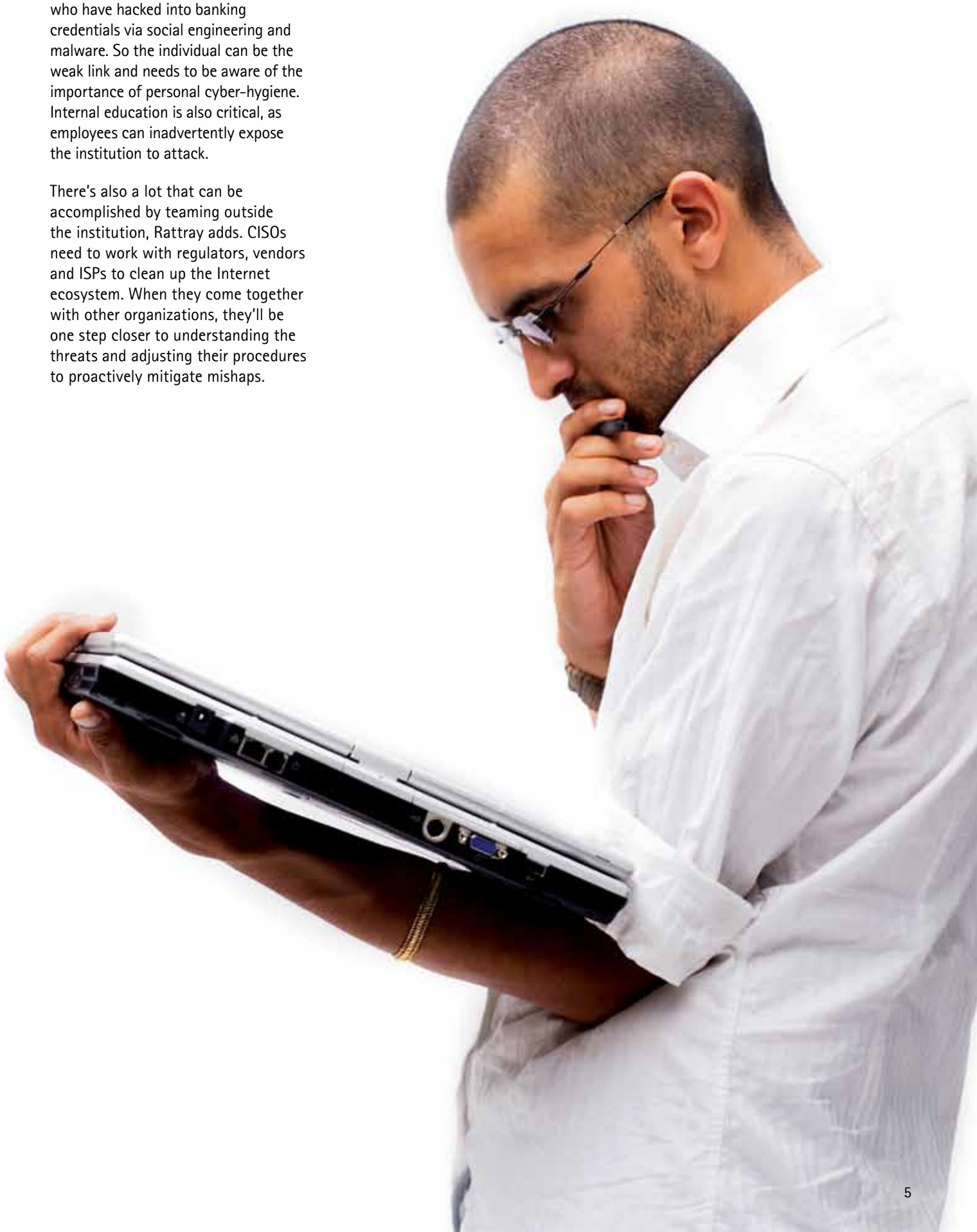
All of these innovations start out as opportunity for institutions—to increase revenue and reduce costs—but threats are evolving as quickly as the opportunities, Rattray laments. "So the question is: Are institutions properly attending to the risk?"

"Banks need to continually work to stay on top of the latest threats, develop sound practices, and implement the right tools to mitigate the risks," Seese advises. "That said, a financial institution's top three security priorities should be education, education, and education."

Many financial attacks target individuals or corporate customers, not banking institutions directly. The dominant model to date has been to steal a person's (or business') credentials or identity, access his bank account, and then take

his money. Through ACH/wire fraud, business customers have lost hundreds of thousands of dollars to fraudsters who have hacked into banking credentials via social engineering and malware. So the individual can be the weak link and needs to be aware of the importance of personal cyber-hygiene. Internal education is also critical, as employees can inadvertently expose the institution to attack.

There's also a lot that can be accomplished by teaming outside the institution, Rattray adds. CISOs need to work with regulators, vendors and ISPs to clean up the Internet ecosystem. When they come together with other organizations, they'll be one step closer to understanding the threats and adjusting their procedures to proactively mitigate mishaps.



Six Practical Steps to Success

When it comes to taking tactical action, Accenture recommends six guiding principles for locking down the institution:

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

Stop thinking in terms of the perimeter. With social networking, mobility, IT consumerization and cloud computing, the enterprise perimeter has become fluid and extremely porous. It is no longer sufficient to button down the perimeter in hopes of keeping the bad guys out. Institutions need to understand their asset topography. Where is the critical information? How is it being accessed? Through what channel and by whom? Take definitive steps to secure those assets directly thus creating a sense of resiliency throughout the organization.

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

Turn security into a culture, starting at the top with specific oversight responsibilities. Accountability is too often blurred across various C-level roles—from the CIO and CISO to legal and risk management—so be sure to identify exactly "where the buck stops." Indeed, the culture must permeate the organization with employee awareness. Make sure everyone understands that the institution is the steward of highly sensitive data. Always take a unified approach with clear policies and common standards across geographic areas and business units.

3. Pay closer attention to applications.

Be sure to extend security to the device and application level. Applications have become a weak link within institutions. Most systems were not built with security in mind, assuming they would reside behind a protected perimeter. But applications have gone mobile, online, and into the cloud. And given today's industrious saboteurs, firewall and anti-virus technology is simply not enough. Trusted application development procedures that incorporate security forethought are a must; as is the ability to measure a specific application's resistance to threat.

4. Check and double-check user identity.

Establish trust in identities. Users must prove they are who they say they are. But today, customer identities are fluid and corporate identities equally elusive. What's worse, identifying information isn't as secret as it used to be. Personal identifiers can easily be found on social networking sites, and hackers are exceedingly proficient at lifting passwords. So carefully think through identity management and authentication. Work toward a program that is cost-effective and non-invasive, yet effective against today's challenges. Leverage advancements in technology—like smartcards and biometrics—which have become more affordable.

5. Get smart about mobile device security.

Make mobility a priority. This growing trend introduces new devices, new operating systems, and of course, new security challenges. Devices are easily lost or stolen, and SIM cards can contain an exorbitant amount of stored personal data. So secure employee and partner devices to protect internal processes. Then educate customers as to the risks and preventative measures—like technology to locate or erase data. And work proactively with carriers to help protect customers.

6. Develop acute situational awareness.

Most importantly, keep ahead of the risks. That starts with a clear understanding of risk across the entire landscape, including the customer environment, partner network, and cloud infrastructure. Assess the impact of that risk on the business. What would a breach to the online statement application do to cost overruns? How would an outage in mobile applications impact revenue? Take measures to manage risk by recognizing backdoor vulnerabilities; identifying chained patterns; expanding the scope of vulnerability testing; leveraging external threat intelligence; and detecting reconnaissance activity. Layer in multiple sources of information—SIEM logs, application scanner results, chatter on blogs, etc. And make very sure partners are operating to the same standards.

Risk vs. Reward

When it comes to making that investment in security, it all comes down to one thing: risk vs. reward.

The reward is glaringly obvious. Innovations like social networking, mobility, IT consumerization and cloud computing promise productivity and efficiency. But most importantly, they offer customers a choice, which ultimately can be a deciding differentiator that directly impacts top-line revenue. Institutions that embrace the trends will flourish—and security is the enabling force behind the opportunity.

But those same innovations open otherwise closed doors to new vulnerabilities—and that risk is a tenuous thing. Obviously, there are non-compliance implications, such as fines, for not managing the risk. But the potential for a breach can be more costly.

Questions Executives Should Be Asking

When it comes to effective cybersecurity, financial services executives must ask the following questions of their teams:

1. Does everyone understand his or her information security responsibilities?
2. Has ownership of, and accountability for, information security been assigned?
3. Does our information strategy allow for the identification, tracking and control of data flow?
4. Have we evaluated our privacy and security technologies for appropriate protections?
5. Have we built a consistent level of awareness among employees?
6. Have we provided the appropriate guidance and training?
7. Are we proactive about spotting patterns that signal internal fraud?
8. Are we choosing business partners with care in terms of their own security posture?
9. Do we have a security strategy for mobile payments and mobile banking?
10. Are we coordinating that strategy with the major wireless telecom carriers?

Rolling Out Cybersecurity

Accenture offers proven strategies and solutions to safeguard financial institutions against an increasingly complex and dangerous threat landscape. Its Cybersecurity Solution was developed with leading industry experts to provide the most innovative approach to security, addressing agencies' current and future computing trends.

Accenture's coordinated approach to thwarting priority threats features proactive measures to protect, deter and pursue attacks. It's a simple way to lock your institution—there's no need to install and manage multiple products—and at the same time create efficiencies for cost savings.

Cybersecurity Resource Library

Articles:

Top 3 Payments Trends for 2011
[[http://www.bankinfosecurity.com/articles.php?art_id=3148]]

PCI Guidance and Emerging Tech
[[http://www.bankinfosecurity.com/articles.php?art_id=3143]]

Incident Response Trends for 2011
[[http://www.bankinfosecurity.com/articles.php?art_id=3134]]

Podcasts:

Scrappy Security for Banks
[[http://www.bankinfosecurity.com/podcasts.php?podcastID=807]]

ATM Fraud: Skimming is No.1 Threat; Phishing Attacks on the Rise
[[http://www.bankinfosecurity.com/podcasts.php?podcastID=862]]

ID Theft: Insider Access Is No. 1 Threat
[[http://www.bankinfosecurity.com/podcasts.php?podcastID=836]]

About Information Security Media Group, Corp. (ISMG)

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focused on Risk Management, Compliance, Fraud, Security and Information Technology. The company provides news, training, education and other related content for professionals in their respective industries. ISMG publishes BankInfoSecurity.com, CUInfoSecurity.com, GovInfoSecurity.com, HealthcareInfoSecurity.com and a variety of other related online properties.

About Accenture

Accenture is a global management consulting, technology services and outsourcing company. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. With approximately 211,000 people serving clients in more than 120 countries, the company generated net revenues of US$21.6 billion for the fiscal year ended Aug. 31, 2010.

For more information on how Accenture can help your organization defend against cyber threats, visit accenture.com/security

ACC11-0018 / 11-2690