Securing Systems in Financial Institutions: Recommendations for Preventing and Responding to IT Security Threats

With attacks leading to losses in the hundreds of millions of dollars, many banks are seeking — and finding — help in the battle against ever-evolving online adversaries.
Securing Systems in Financial Institutions: Recommendations for Preventing and Responding to IT Security Threats

With attacks leading to losses in the hundreds of millions of dollars, many banks are seeking — and finding — help in the battle against ever-evolving online adversaries.

By Peggy Bresnick Kendler

Financial institutions continue to face pressure to comply with regulatory mandates, address changing customer demands and keep costs down. At the same time, they must secure networks, applications and data against increasingly sophisticated criminals. Firms that fail to meet any one of these significant challenges risk falling behind in a highly volatile market. And, if they can’t secure systems and data from Trojans, malware, distributed denial of service (DDoS) attacks and other cyber threats, they face widespread business disruption as well as significant financial and reputational damage.

Not surprisingly, then, cybersecurity is a top concern for financial institutions, especially as more and more transactions occur via online channels. According to the Ponemon Institute report “2012 Cost of Cyber Crime Study: United States,” the average annualized cost of cybercrime varies by industry segment, with financial services, defense and utilities and energy organizations experiencing substantially higher costs than other segments. Ponemon Institute research shows that the average annualized cost of cybercrime for financial services organizations amounted to $16.44 million in 2012, up more than 11 percent from 2011 costs.

The costs of a security incident (unauthorized access of data, applications and systems by circumventing security measures) can be very steep. If a data breach occurs and personal information gets into the hands of a malevolent hacker, the financial costs of dealing with such a breach — communicating with customers after the fact, or payouts due to lawsuits, for instance — can be astronomical. But that’s not all — the organization could also face fines and penalties if the breach resulted from noncompliance with the ever-tightening regulatory mandates that demand security measures to protect sensitive information.

It can be challenging for banks to know where personal and account data resides, or where the holes in their security strategy are. But banking information of all types is supremely valuable to hackers who work to stay ahead of corporate security protection efforts. In addition to ongoing individual attacks, criminals are targeting banks in increasingly sophisticated ways through what’s known as “advanced persistent threats.” These are cybercrimes that are executed methodically over a period of time against a specific organization or entity. Although these can be politically motivated, they are also commonly used for financial gain or to steal intellectual property. The criminals behind these advanced threats use many different tools and mechanisms to accomplish their goal. A whole underground economy revolves around stolen customer information, and

ABOUT THE AUTHOR

Peggy Bresnick Kendler has been a professional writer for the past 30 years. She has worked on a wide variety of special projects on behalf of some of the most familiar companies in the financial technology field.
the wide network of malevolent individuals motivated by greed has become very difficult to fight.

The 2012 Ponemon Institute report on cybercrime found that 90 percent of organizations in its study experienced leakage or loss (or both) of sensitive or confidential documents over the preceding 12-month period. And companies reported 1.8 successful attacks per company each week, representing an increase of 42 percent from last year’s study.

Maintaining adequate data security has become very challenging for investment firms and banks, which must grapple with a widening array of security issues, including:

**Safeguarding online banking.** Despite the perils of the cyberworld, financial institutions must provide an array of personalized online services, because customers increasingly demand them. Although online self-service and transaction options may offer significant savings over traditional call centers, they also introduce new challenges to keeping customer information private.

**Protecting mobile banking.** According to the Pew Internet and American Life Project, a project of the Pew Research Center, more than eight in 10 adults (85%) in the U.S. owned cell phones as of November 2012 and, as of mid-2012, nearly half (46%) of all American adults owned smartphones.

Mobile banking has made it easier than ever for customers to do business with their financial institutions. Consumers are increasingly using their phones and tablet devices for tasks such as checking balances, transferring funds and paying bills. According to Javelin Strategy & Research, mobile banking gained 10 million new users in 2012 and currently reaches about a third of the mobile adult U.S. population. And according to the Pew Internet and American Life Project, 29 percent of all cell phone owners currently use their phones to check bank account balances or do online banking, a marked increase from 18 percent of users in 2011. A full 45 percent of young adults ages 18 to 29 years old are using their mobile phones for online banking. In its “The State of Mobile Banking 2012” report, Forrester Research predicts that the number of U.S. mobile banking users will actually double in the next five years to reach 108 million by 2017, accounting for about 46 percent of U.S. bank account holders.

But with that convenience comes more risk. Because mobile devices can lack the security functions that PCs offer, they can be easier channels for criminals to compromise, enabling them to gain access to stored data.

**Securing applications.** Computers and mobile devices are easily compromised and tempting targets for malicious software. Yet it’s not just the devices themselves that must be secured; banks must also secure a multitude of Web and mobile applications. These include applications across many different platforms used for cash transactions, deposits and trading, all of which must be secured and audited. Banks must also demonstrate and document safety and security measures to meet regulatory requirements.

**Combating internal threats.** Not only do investment firms and banks need to protect themselves from threats coming from outside the organization, they also need to prevent leaks of internal information from employees, contractors and partners. According to Deloitte’s “2012 DTTL Global Financial Services Industry Security Survey,” nearly half (49%) of surveyed organizations said they actively manage vulnerabilities. More than four in five (82%) of these firms said they are also actively researching new threats to proactively protect their environment from emerging threats. However, only about 40 percent of respondents said they were very confident that their organization’s assets are sufficiently protected from an attack or breach – and only about one in five (21.3%) said they were similarly confident about their ability to protect information assets from an internal attack or breach.

**Achieving regulatory compliance.** While there are already several standards financial institutions must meet — including Payment Card Industry (PCI) Data Security Standard (DSS), Graham-Leach-Bliley Act (GLBA), and Sarbanes-Oxley — new guidance and regulations are introduced on a regular basis.

The 2011 supplement on Internet Banking Authentication, an update of the 2005 Federal Financial Institutions Examination Council (FFIEC), provided recommendations on how financial
firms should use multifactor authentication, regular policy reviews and risk assessment for securing online systems. However, many industry experts believe the measures are already outdated given the increased complexity of threats.

**Meeting customer expectations.** Banking customers, who are increasingly conducting business via their computers and mobile devices, have also become a primary target for attackers. And aggravating the concerns, attackers are using very sophisticated techniques to detect vulnerabilities in not only in financial institutions’ systems, but also in their customers’ systems.

With security breaches appearing more frequently in the news, consumers understand the importance of keeping their personal information secure — and they expect their financial institutions to safeguard their information. Fraud-prevention capabilities are increasingly becoming a competitive differentiator for financial institutions.

**Protecting intellectual property.** Like organizations of all types, financial firms want to ensure their intellectual property isn’t compromised. Cybersurveillance — monitoring the Internet to make sure sensitive information hasn’t been leaked — can give financial firms a measure of security, although the monitoring activities can be costly and difficult to do successfully. It is much more prudent and cost-effective to protect information than to try to track it after the fact.

**Financial Firms Are on the Right Track, But Not All the Way There**

In general, many large financial services organizations have implemented advanced security measures and are leaders in technology implementation. Many have robust and comprehensive security standards and policies in place and are able to execute and document their strategy. But they’re not always confident that the security they have in place is adequate to protect their systems and sensitive information.

According to Ernst & Young’s 15th annual Global Information Security Survey report, released in November 2012, most survey respondents across industries are taking steps to enhance their information security capabilities, although few are keeping up with the ever-evolving risk landscape. A full 80 percent of respondents believe that there is an increasing level of risk from increased external threats. Indeed, more than three-fourths of respondents (77%) said they have seen an increase in external threats that include hacktivism, state-sponsored espionage, organized crime and terrorism.

The report notes that although organizations are aware of the need for greater security protection, they are often unable to keep up with the growing scope and size of threats. Clearly, there is a large and increasing gap between security protection and security threats that leaves organizations vulnerable to cyber-attacks.

**Solutions for Financial Institutions**

Although most large banks and investment firms are doing at least an adequate job in securing networks and applications, many could use help in protecting themselves from malicious attacks and augmenting the provisions they already have in place. However, these organizations vary in terms of their willingness to hand off security responsibilities. Some firms are very protective of their information — they won’t let an outside provider see their data and don’t feel comfortable delegating monitoring responsibilities to a security service provider. Although these organizations may have clarity concerning their own environment, they lack the global visibility, exposure and experience with evolving security threats that an outside security services provider can offer.

Other financial firms may be comfortable doing their own security in-house, but may also be open to a third-party managed services provider to do some network monitoring, oversee their most critical perimeter devices and help protect core assets. This hybrid approach can be highly effective and can result in considerable savings of both cost and resources. And some organizations, particularly smaller to mid-size banks and credit unions, look to managed security services providers to comprehensively perform all security tasks.

A November 2011 report from Aite Group, “CIO Survey 2011: Eight IT Habits of High-Performing Banks,” identifies investment in IT solutions, mobile banking and strategic outsourcing to banking technology vendors as key characteristics of high-performing banks that had a greater return on operating capital, equity, and
assets. As outsourcing providers enhance their offerings, more banks are embracing outsourcing, not only to save money, but to gain access to better technology.

While the larger for-profit banking sector is typically very advanced in terms of security, smaller banks and credit unions may lag behind. Because they’re driven by regulatory bodies, all financial firms tend to have a reasonably good baseline. But these smaller firms struggle with the expense and difficulty of implementing cutting-edge, best-practice security measures. Security isn’t a core business for financial firms, and doing it right can be challenging. Banks and investment firms need a way to cost-effectively protect themselves from evolving threats with a best-of-breed approach.

**Looking for Help**

For many banks, the solution is to tap the expertise of a security vendor that can bring proven solutions that address financial institutions’ most critical security challenges.

One of the leading providers to the banking industry is Dell SecureWorks, which provides a range of information security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs. Dell SecureWorks works with banks’ IT departments, creating a partnership and an augmentation of the IT team to optimize each institution’s security efforts, create efficiencies and facilitate regulatory compliance. Using a flexible delivery model, Dell SecureWorks security services provide protection across the network, safeguarding the perimeter as well as critical internal assets, data, remote users, customers and partners. Its services are vendor-agnostic and can assimilate easily into a bank’s existing environment.

---

**Dell SecureWorks in Use**

Dell SecureWorks information security services can provide financial services firms with significantly improved security. A TechValidate poll of 349 financial services clients found that 89 percent of these institutions rated their overall security posture as “stronger” or “better” since they engaged Dell SecureWorks as a security services vendor.

Examples of successful Dell SecureWorks customer engagements include:

- **A Fortune 500 financial services company** seeking additional security expertise, better operational efficiency and improved regulatory compliance tapped Dell SecureWorks to comply with a variety of standards, including PCI Data Security Standard, GLBA, FFIEC Guidelines and Sarbanes-Oxley. The financial services firm reports that it has realized up to 19 percent in cost savings with Dell SecureWorks Security Services compared to performing the same security functions with in-house staff and tools, and that its overall security posture is much stronger since engaging Dell SecureWorks.

- **A large enterprise bank** implemented Dell SecureWorks Security Services for 24/7 security coverage, to improve quality of protection, to provide additional security expertise and to improve compliance with regulatory mandates. In addition, the firm offloaded its resource-intensive security tasks to Dell SecureWorks Security Services and improved faster response to threats. As a result, the firm reports savings of 80 percent compared with the cost of performing the same security functions with in-house staff and tools.

- **An S&P 500 financial services company** was able to solve its security and operational efficiency challenges with Dell SecureWorks Security Services, while reducing overall costs. Dell SecureWorks provides the financial firm 24/7 security monitoring, improving the overall quality of protection and providing additional security expertise and making the firm more responsive to threats. In addition, the solution increased operational efficiency.
Dell SecureWorks offers a comprehensive suite of services, including

- Managed information security services
- Security information and event management (SIEM and SIM On-Demand)
- Security and risk consulting
- Compliance solutions including PCI, GLBA, FFIEC, HIPAA and others

**Guarding Against Shifting Threats**

Financial services organizations of all sizes and types and in all locations must protect themselves from cyber threats. No longer are network attacks and theft of sensitive information perpetrated by individuals for their own amusement; cyber attacks against financial services firms today are typically carried out by large and often sophisticated criminal organizations. These entities are skillful, stealthy and adept at attacking banks at their most vulnerable access points. But the full range of threats is increasingly diverse. Not only must financial services companies protect against external data breaches, they also must prevent data leaks by employees, whether through intentional theft, lost or stolen devices, or accidental exposure.

For financial services firms, the need for comprehensive information security is more critical than ever, and failing to address this urgency can invite a host of severe consequences, including fines, brand damage, and financial losses. Financial firms that don’t bolster the security provisions with financial resources might find that they are playing a game of roulette with their business — and they stand to suffer huge costs and headaches and irrecoverable losses to their brand and reputation in the event of a security breach.

Although top-of-mind for most financial services firms, cyber security is usually not a core competency. For that reason, many financial organizations find that a partnership with a service provider can supply them with optimized network security solutions, ongoing threat intelligence and comprehensive endpoint security that are critical to protect against current and emerging threats.

*For more information on Dell SecureWorks, visit [www.secureworks.com](http://www.secureworks.com) or call 877-905-6661.*