Show me the money

Are cyber attacks damaging client trust to the breaking point?

July 2009

A publication of the PricewaterhouseCoopers' Financial Services Institute (FSI)

PricewaterhouseCoopers

Table of contents

Section 1 – Point of view

Section 1 – Point of view

Alarming headlines of data breaches appear almost daily

This is a serious, costly issue. Recent headlines include:
“Financial Crimes are Getting More Sophisticated” – American Banker, June 30, 2009
“Malicious Attacks Most Blamed in ’09 Data Breaches” – The Washington Post, June 19, 2009
“Obama Set to Create 'Cyber Czar' Position” – The Wall Street Journal, May 29, 2009
“Data Breaches Cost Businesses More” – The Wall Street Journal, February 2, 2009
“Data Breach Causes Shareholder Value Decline” – USA Today, January 30, 2009
“Payment Process Breach May Be Largest Ever” – The Washington Post, January 20, 2009
“Data Manager of Japanese Brokerage Steals Data on 1.5 Million, Sells to Marketers” – The Bureau of National Affairs, January 29, 2009
“Cyber-Scams on the Uptick in Downturn” – The Wall Street Journal, January 29, 2009
“Data of 1.5 Million Exposed in Hacking at U.S. Processing Arm of Foreign Bank” – The Bureau of National Affairs, January 5, 2009

Section 1 – Point of view
Cyber breaches are becoming more common

Both the number of reported breaches and the number of associated breached records have increased in recent years.

From 2007 to 2008, as reported by the Identity Theft Resource Center, the number of breaches in the credit, banking, and financial industries increased from 31 to 78, a 150 percent increase. The number of breached records increased from 8.8 million to 18.7 million, a 112% increase.[1]

Most financial services organizations are at risk because of their global operating model.

The complex structure of financial services organizations and the global, interconnected marketplace in which they operate make it difficult to effectively track and manage data. Additionally, the use of third-party service providers makes traditional protection methods such as perimeter controls less effective, resulting in inadequate measures to protect sensitive data. The following statistics highlight the degree to which financial services are at risk:

- Fifty-four percent of financial services organizations do not have an accurate inventory of where personal data for employees and customers is collected, transmitted, and stored.[2]
- Ninety percent of ethical hacking attempts by PricewaterhouseCoopers (PwC) were successful at gaining access to highly sensitive information.

[1]Source: The Identity Theft Resource Center 2008 Breach Report; results for the banking/credit/financial category.
[2]Source: PwC's 2008 Global State of Information Security Survey, conducted with CIO and CSO magazines.

Section 1 – Point of view

Cyber breaches are becoming more sophisticated, and new threats are emerging

Cyber threats are gaining in sophistication.

Not only are the stakes higher, but the adversaries have also upped their game.

Better organized and technologically savvy criminals are targeting larger amounts of sensitive information, including information that leads to theft of funds. Protecting sensitive personal financial information has become more challenging in light of:

- Increased electronic transactions
- Outsourcing of transaction processing functions
- More sophisticated penetration tools used by hackers and identity thieves

The technical sophistication of attacks continues to increase as skillful resources in Asia and Eastern Europe have been and continue to be attracted by lucrative returns from recent cyber attacks. Ninety-five percent of records compromised are the result of attacks involving advanced skills, significant customization, and/or extensive resources. Additionally, organized criminal groups account for 91 percent of records compromised.[1]

New threats continue to emerge.

New methods and types of cyber attacks continue to be developed by cyber criminals. In a denial-of-service (DOS) attack, clients and customers cannot perform expected transactions or access online account information. Similarly, distributed-denial-of-service attacks occur when attackers leverage an extended network of global devices (known as bot-nets) to conduct denial of service attacks against multiple organizations simultaneously. These types of attacks are becoming more prevalent and may result in lost customer confidence and reputational damage. For some financial services organizations, especially ones that offer online transactions and processing, a DOS attack may result in brand damage equal to that of a data breach.

[1]Source: 2009 Data Breach Investigations Report (Verizon Business RISK Team)

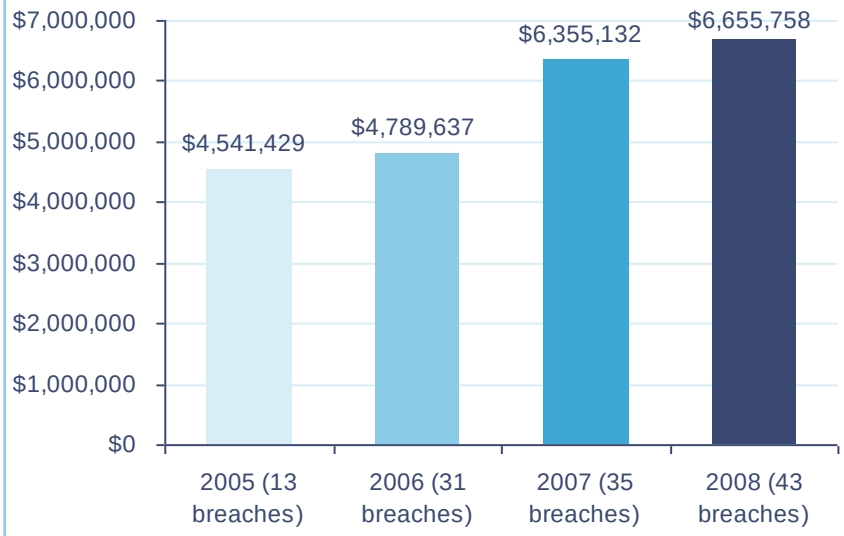
Section 1 – Point of view

Response and remediation costs continue to rise

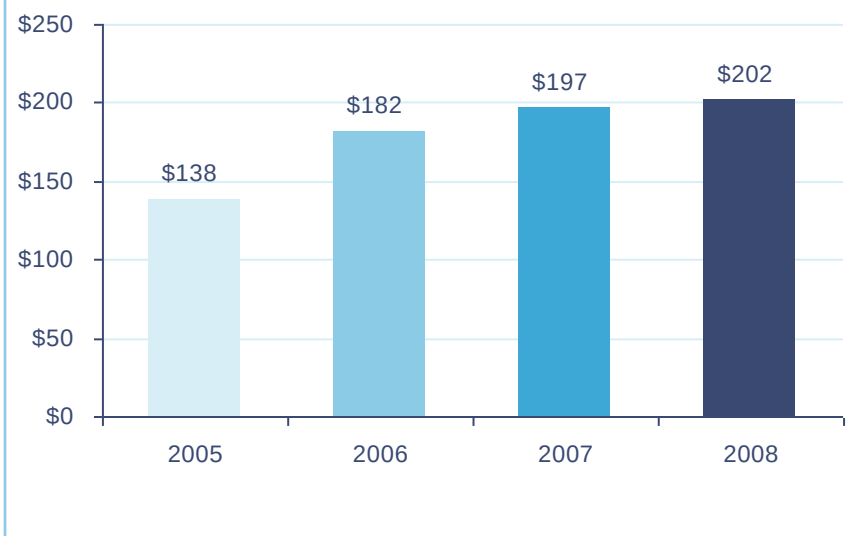
Costs for responding to and remediating issues related to data breaches run into the millions of dollars. According to the Ponemon Institute, which surveyed actual data breaches from 43 US companies across a range of industries, the average organizational cost for a data breach in 2008 was $6.6 million.

Organizations which build their brand on trust and engage third parties have more to lose from a data breach. The cost of lost business now accounts for 69 percent of data breach costs, up from 65 percent in 2007. Additionally, the per-victim cost is $52 higher if the breach happened at a third party ($231 versus $179).

Average organization costs of a breach



Average per-record cost of a breach



Source: 2008 Annual Study: Cost of a Data Breach (Ponemon Institute).

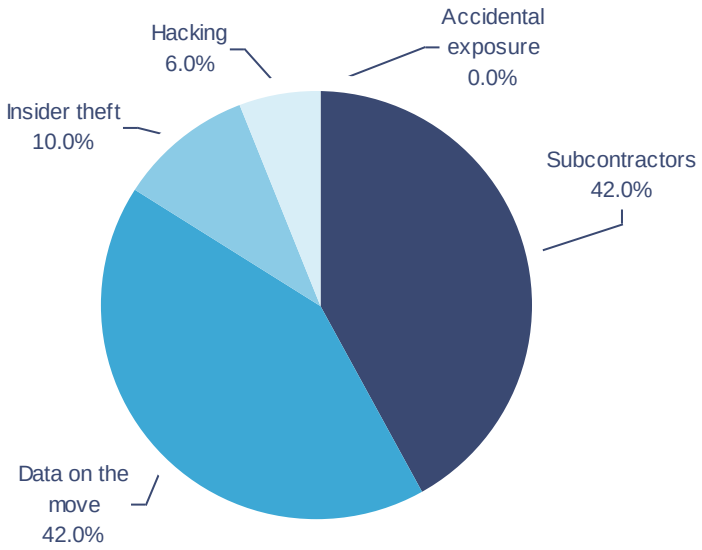
Section 1 – Point of view

Breaches are overwhelmingly electronic and tend to occur when data is in motion or in the hands of subcontractors

Data breaches in 2008:

- Over 99 percent of reported breaches in the credit, banking and financial industries involved electronic records (only 482 of 18 million breached records were paper).[1]
- Most breaches in the credit, banking and financial industries were the result of data in motion or data in the hands of subcontractors.[1]
- Sixty-six percent of financial services respondents in the PwC Global State of Information Security 2008 survey stated that their firm does not have an inventory of all data, including that held at third parties handling personal data of employees and customers.[2]
- Insider theft was cited as the source in 10 percent of reported breaches.
- Only 2.4 percent of breaches occurred when encryption or other strong protection methods were in use.[3]

Sources of data breaches[1]



[1]Source: The Identity Theft Resource Center 2008 Breach Report; results for the banking/credit/financial category.
[2]Source: PwC's 2008 Global State of Information Security Survey, conducted with CIO and CSO magazines.
[3]Source: The Identity Theft Resource Center 2008 Breach Report; results for all categories.

Section 1 – Point of view

Financial services institutions are particularly attractive targets

All financial services companies and customers are vulnerable to data security breaches.

Over 262 million known records of US residents have been exposed to data breaches since 2005.[1] In many more cases, the number of records compromised is never reported on and may never be truly known. Prevention of data breaches is hindered by a lack of a complete data inventory. Evidence shows that the majority of companies have an incomplete knowledge of where their critical data resides and how susceptible it is to theft. Additionally, many organizations rely on third parties to store, access, process, and secure critical data, which amplifies their risk.

Financial services institutions are explicit targets, and attacks against them and their customers continue to intensify. Attackers have had recent success using customer account and ATM card fraud in order to directly steal funds. These criminals continue to search for any electronic doorway allowing them to gather customer personal and account information. Access points include databases and applications that may not be considered part of the direct financial transaction chain such as informational Web sites and other systems connected to and now managed via the Internet.

[1]Source: Privacy Rights Clearinghouse, http://www.privacyrights.org/ar/ChronDataBreaches.htm# Total, as of June 23, 2009; accessed June 26, 2009.

Section 1 – Point of view

Old approaches and responses to cyber risks will need to be fundamentally reexamined

Regulation, financial impact, and major incidents will all contribute to a "day of reckoning," which will elevate this issue to the CEO and board level.

Until now, financial institutions have not experienced widespread severe financial or reputational damage as a result of data breaches. As such, it has not become a CEO issue. However, it is our view that this is likely to change, because of factors such as the increasing sophistication of cyber attacks, the growing possibility of sovereign involvement in future attacks on the financial infrastructure of the United States, and the continuing growth of identity theft. A "day of reckoning" will emerge, driven by the following factors:

- Regulation – the impact of identity theft and cyber breaches on the consumer will become so severe that regulators and politicians will focus additional attention on these issues
- Financial impact – loss of clients and/or curtailment of transactions (such as purchases on the Internet) will increasingly impact those institutions that fail to retain customer trust
- Other major incidents – the publicizing of a future major incident contrasts with past incidents that were not reported in the public domain. It is only a matter of time before such an incident, perhaps involving a foreign government, is perceived to threaten either the stability of a particular institution or the financial system as a whole.

Section 1 – Point of view

Regulatory focus on consumer/customer data will only intensify

A unique set of regulatory and other external pressures on financial services companies places an additional burden on these institutions to protect the data with which they are entrusted. At the same time, new laws and regulations continue to emerge with the aim of strengthening consumer and business protection.

Financial services companies operate in one of the most highly regulated industries and must comply with multiple requirements imposed by various levels of government. In the United States, 44 states have instituted data breach notification statutes, some of which have provisions for fines and sanctions.[1] From the SEC, FTC, and Federal Financial Institutions Examination Council (FFIEC), to industry standards such as PCI, many stakeholders play a role in ensuring compliance. However, compliance with regulations alone may not provide sufficient protection against security breaches. When things go wrong and a breach occurs, there are often a large number of external parties with a legal right and obligation to determine the cause and the resulting consequences.

Financial services companies increasingly host and use data that criminals target. By breaching data on banking, investments, credit cards, and payments, criminals can assume the identity of customers to make illegal purchases. As criminals become more sophisticated and gather more data, the type of transactions that they are able to complete becomes more advanced. As a result, it is critical to adequately protect methods of money transfer such as wire applications, ATM applications, and automated clearing house applications.

Traditional security-focused protection methods are often not sufficient to safeguard sensitive financial data. The appropriate defense requires a coordinated effort among corporate groups focused on security, privacy, fraud prevention, and records management, with heavy cooperation and understanding from the business units that own the data and the regulatory/legal department.

Additionally, there are many outstanding questions as to how identity theft and data protection may be incorporated into President Obama's proposed Consumer Protection Act, as well as questions about the potential increased role and responsibility of the FTC with respect to the protection of personally identifiable information. This focus by the US government serves as more evidence that the regulatory focus on consumer/customer data protection will only intensify.

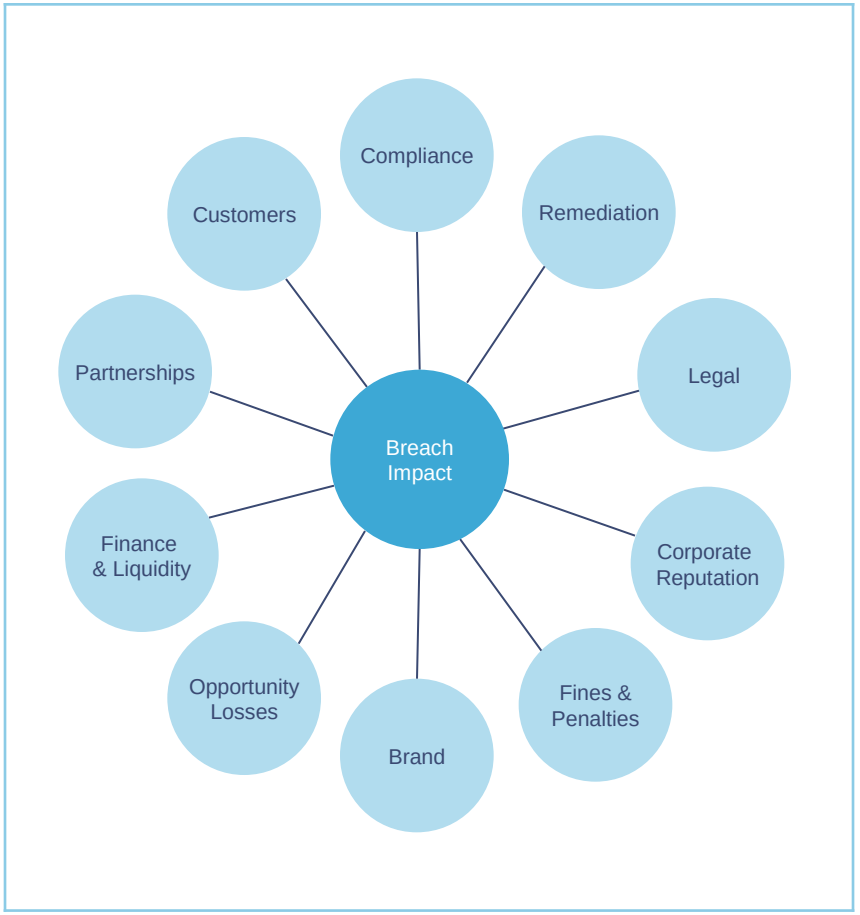
[1]Source: National Conference of State Legislators, http://www.ncsl.org/Default.aspx?TabId=13489, summary of state security breach notification laws as of May 26, 2009; accessed June 26, 2009.

Section 1 – Point of view

Perception is reality – erosion of trust will likely lead to negative revenue impacts

Financial institutions that fall victim to cyber attack, theft, and/or loss may lose more than just their data.

- Perception is reality — any loss of data can result in loss of trust by customers and employees, and with that, loss of business. Insufficient data protection and privacy controls can result in significant costs for response and remediation associated with data breaches, lawsuits, erosion of future revenue, loss of brand reputation and customers, government fines, and new regulation.
- Embracing data protection and privacy as an integral component of their operations may enable financial services companies to acquire a competitive advantage by reducing their own risk of financial loss and reputational damage.
- Customers rely on financial institutions to safeguard their assets, personal information, and identities. The recent growth in identity theft has not yet had a marked impact on key revenue streams for financial institutions such as debit card usage and Internet payment transactions. However, if attackers continue to succeed, these revenue streams will likely be negatively impacted.



Section 1 – Point of view

A new approach to cyber protection is required

Companies should develop a thorough approach to cyber protection and fraud prevention. This approach should continuously prepare for and respond to potential threats and remediate breach risks.

Cyber security initiatives that are narrow in scope are ineffective at recognizing and addressing the risks across the broader organization. In order to fully assess an organization's cyber threats and risks, a detailed understanding of the location, protection, transaction flows, and breach exposure of sensitive data must be obtained. In our experience, organizations typically spend more time and effort responding to data breaches, rather than focusing on trying to avoid a breach altogether.

As a result of prior data breaches and regulatory requirements, many companies have started protecting data at the element level in addition to the system and application level. Furthermore, companies have begun proactively inventorying locations of high-risk personal and financial information collection, storage, and use. Because of the tremendous downside of a data breach, organizations should, and are, shifting from a reactive mind-set to a proactive approach.

Companies should develop a thorough approach to cyber protection and fraud prevention. This approach should continuously prepare for and respond to potential threats and remediate breach risks. It should also take into account the lifecycle of information handled by employees, vendors, and consumers and should be sufficiently flexible to allow upgrades without placing a significant burden on end users.

Therefore, cyber protection should be placed within the top tier of a company's priorities and budgeted appropriately. A company's board of directors should assess the cyber protection of the company with as much rigor as it does other processes within the organization.

Section 2 – Competitive intelligence

Section 2 – Competitive intelligence
Leading versus observed practices

The following tables illustrate the difference between leading practices and what we see in the industry.

Industry leading practices	Global bank	Broker-dealer firm	Alternative investment firm	Credit card processing firm
An integrated approach, supported by senior management, to a comprehensive cyber security program that is supported by management and is centrally developed and managed. It includes relevant regulatory compliance requirements, vendor management procedures, and training and awareness steps.	• Central DP office cataloging requirements in all countries of business • Reviewing every application against known requirements and ensuring the local countries are complying • Providing first draft C2C agreements and other legal documents that are necessary • Slightly siloed approach lacking buy-in from all businesses	• Lack of comprehensive integration • Little business buy-in • Some management support • Moving toward sitting at the same table as the business groups • Centrally developed vendor oversight group that sat at the table with CTO	• Looking at data of customers and employees and mapping it to regulations in each country • No dedicated privacy officers • Currently developing data privacy policies	• Compliant with PCI DSS • Resources assigned to privacy function as part of a larger overall job responsibility • Developed and released data privacy policies • Annual testing completed to ensure that data is being safeguarded

Section 2 – Competitive intelligence
Leading versus observed practices (continued)

The following tables illustrate the difference between leading practices and what we see in the industry.

Industry leading practices	Global bank	Broker-dealer firm	Alternative investment firm	Credit card processing firm
Cyber security analysis and monitoring of transaction, network, and application environment with processes and solutions in place to assist in breach and attack (DOS) prevention and identification. This includes analysis of electronic data theft from third-party and contractors' devices per above.	• Security team coordinated and sharing with fraud team on transaction anomalies • Segmented networks by business function, i.e. segmented wire transfer, payment, and core transaction processing environments • Data loss prevention monitoring in place on sensitive data leaving the environment and core applications and databases within the environment • External and internal intrusion prevention, web-based application protection implemented • Multiple diverse network connections are established with automatic monitoring and switching if DOS attacks are detected	• Security team not coordinated with any internal transaction monitoring • External data loss prevention implemented as well as external intrusion prevention • External network segmentation in place but no internal network segmentation or malicious traffic monitoring	• Security team is beginning to coordinate with transaction monitoring and trade compliance • Segment internal and external networks with malicious content and e-mail filtering from Internet and between departments • Data loss prevention monitoring in place for outbound data focused on sensitive and trade data • Leading industry system administration and trading monitoring. All system administration and trading activity is captured and logged via multiple methods, such as key logging and screen scraping.	• Minimal cyber risk analysis coordination among internal teams • Minimal network segmentation and traffic analysis at any level • Web application protection and logging at different network segments

Section 2 – Competitive intelligence
Leading versus observed practices (continued)

The following tables illustrate the difference between leading practices and what we see in the industry.

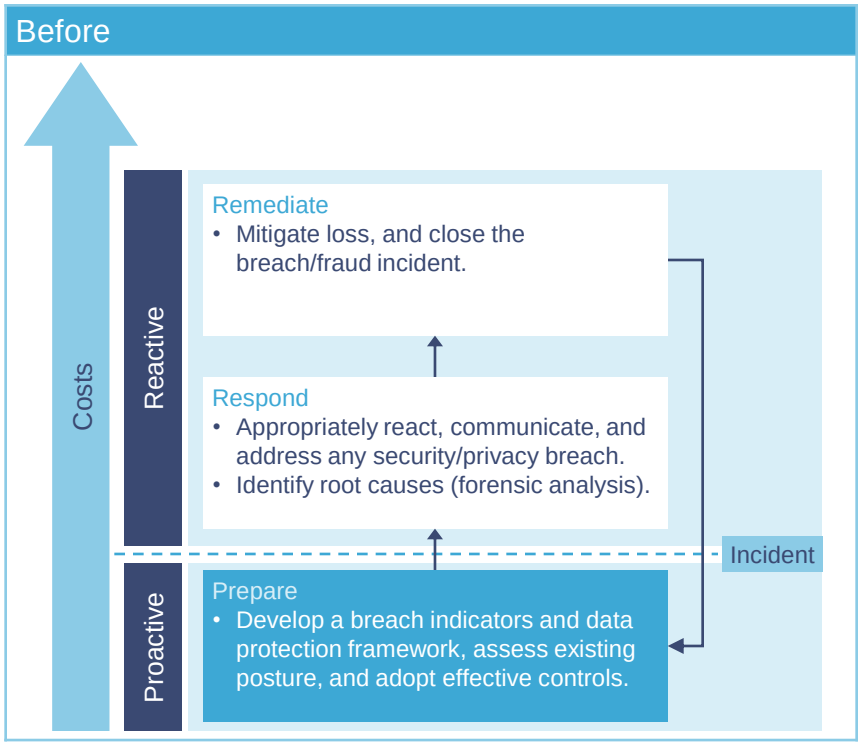
Industry leading practices	Global bank	Broker-dealer firm	Alternative investment firm	Credit card processing firm
Fully developed crisis and incident response program that has management buy-in, has been legally reviewed, and is periodically tested. The program has centralized communication functions that identify when and to whom notifications need to be made. Additionally, retention policies are in place, and a data inventory has been performed to facilitate e-discovery.	• Fully developed crisis and incident response program including communication functions • Dedicated Information Security Office • Representatives from all business units • Incomplete data inventory because of a large amount of applications	• Ad hoc monitoring of the environment and responding to incidents • Security and privacy issues were not high on the list for business • Audit issues were high priority • Communication functions not fully centralized • Moving toward integrated incident management database across groups • Robust forensic unit with respect to infrastructure • Seven-year rule retention policy	• No formalized program; utilizes ad hoc processes for response • No IT representatives responsible for incident response • No dedicated full-time employees for incident management • Established relationships with security vendors for support • Informal communication program plan • Saving and logging files, not monitoring • Implemented legal hold procedures • Implementing document retention program	• Developed crisis and incident response program • Communication functions not fully centralized • No dedicated full-time, but identified, employees for incident management • Established relationships with security vendors for support including forensic capabilities

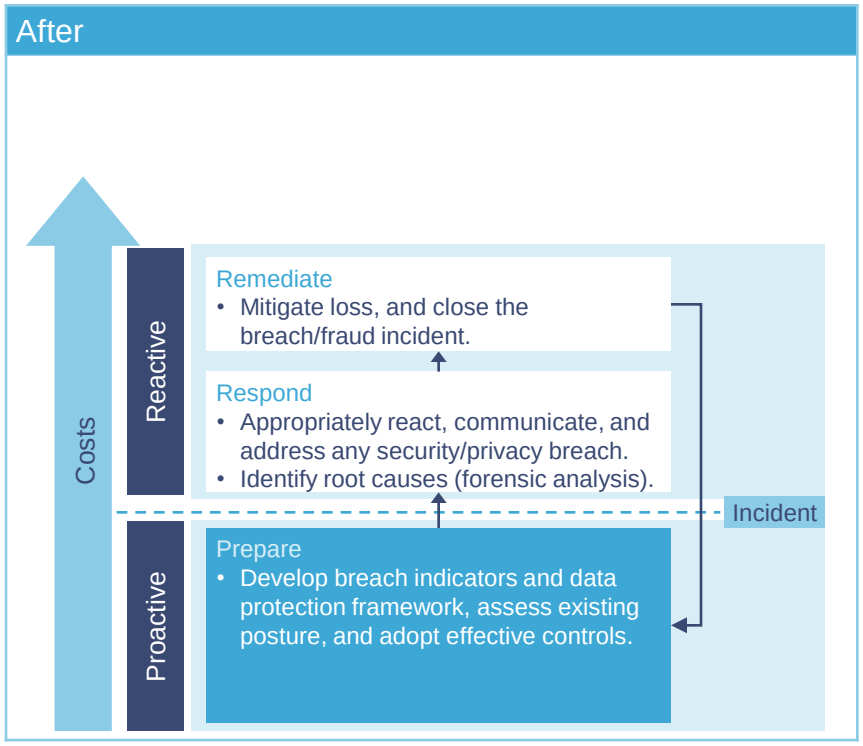
Section 3 – Framework for action

Section 3 – Framework for action

By taking more proactive cyber breach measures, companies can significantly reduce the overall likelihood and resulting cost of a breach.

Continuous evaluation and enhancement of cyber breach protection and response capabilities will enable an organization to spend less time responding to and remediating breaches. Companies without adequate security and breach risk management procedures had breach costs of 19 percent (or $35 per record), higher than those with adequate procedures.[1]





[1]Source: 2008 Annual Study: Cost of a Data Breach (Ponemon Institute).

Section 3 – Framework for action

Approach focuses on identifying and preventing breaches and protecting sensitive data.

Traditionally, financial services companies have focused on performing risk and controls assessments on base technology infrastructure, but not combining those efforts with a detailed data inventory and a transaction and breach indicator analysis.

Define sensitive data	Inventory sensitive data	Information risk & controls assessment	Fraud & breach indicator analysis	Risk prioritization & remediation
• Define data elements that are deemed sensitive from a business, customer, and regulatory perspective • Elements include traditional personally identifiable information (PII) and account information, but can also include intellectual property such as: - Source code - Trading algorithms - Portfolio management methods - System administration details	• Identify locations where the sensitive data resides within the environment • Include both physical and electronic forms of data in this step • Identify all sensitive data locations for structured data • Identify all sensitive data locations for unstructured data • Risk rate sensitive data inventory based on threats	• Assess policy and procedural controls in place that are protecting data elements • Assess technical controls in place protecting key infrastructure that hosts or transmits sensitive data • Assess fraud monitoring and detection capabilities that are in place for transactions involving sensitive data • Identify where gaps exist between implemented controls	• Analyze transaction data for indications of malicious or abnormal activity • Analyze captured system data for indications of a breach such as root kits, malware, and memory resident programs that traditional protection methods, such as anti-virus, do not detect • Analyze network traffic for abnormal or malicious activity such as unusual amounts of data transfer, abnormal data transmission methods, or communication with known malicious networks	• Evaluate threats to the environment • Prioritize resulting gaps from prior work streams to understand where the highest risk areas reside • Develop remediation strategy based on threats, risks, and available spend, including potential design and implementation of new breach protection processes or technology • Remediate based on road map • Continuously reassess the environment using the method

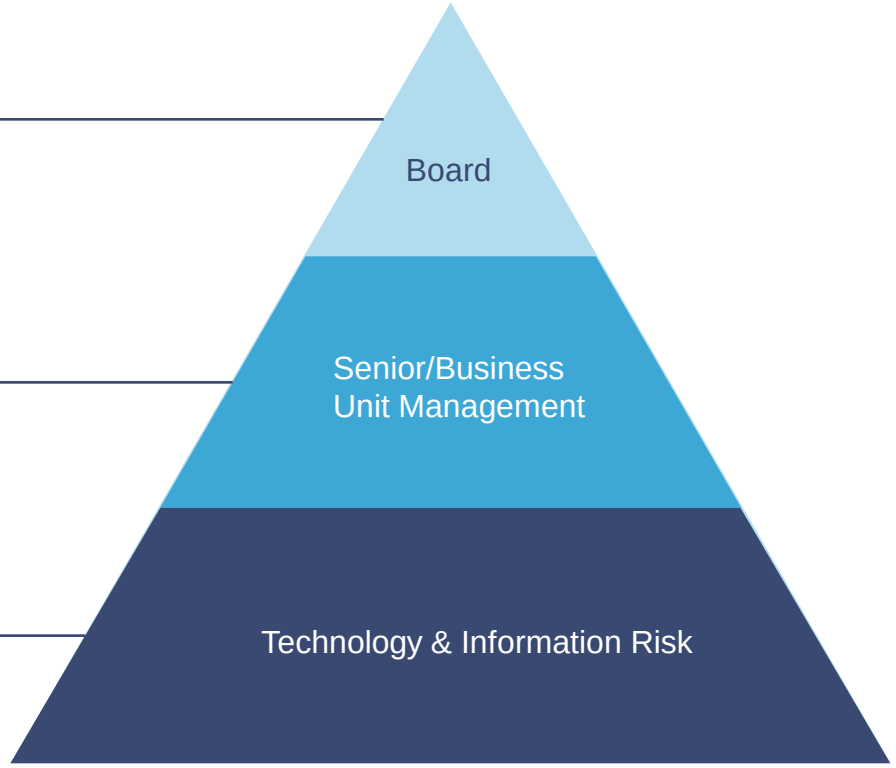
Section 3 – Framework for action

Governance and reporting model framework foundation

Direct and support management processes, policies, and procedures to protect the institution from cyber attack

Oversee the implementation of the cyber protection strategies and communicate those strategies to stakeholders

Manage day-to-day activities, conform with guidelines set by executive committee, and raise key issues for further consideration



Section 4 – How PwC can help

Section 4 – How PwC can help
PwC's background

Global Financial Services Security & Privacy Capabilities

- PricewaterhouseCoopers is the leading service firm in the financial services industry with regard to privacy and security expertise. Our Privacy and Information Security practice includes more than 1100 professionals in the United States alone and 2,900 around the world fully dedicated to information security, providing a broad scope of security and privacy expertise and deep technical knowledge. Our practice is dedicated to providing our clients world-class security advice, including strategy, design, implementation and assessment services. A large dedicated practice of this size allows us to regularly meet with the industry analysts and vendor partners to shape the future direction of the security landscape.
- PwC has made significant investments in the information security industry in the form of security roundtables and long-term partnerships with leading vendors. In fact, our commitment to this industry is so well-known that new technology vendors regularly come to us to assess their products and help drive them into the marketplace. Additionally, our security practice is known internationally for its experience and strong security skills in threat and vulnerability management, cyber crime prevention, response and recovery, strategy and security design, and implementation services.
- PwC is also a thought leader in information security, and is frequently involved in the publication of authoritative books and white papers on information security. This includes:
  - Information Technology: A Strategic Guide for Business
  - Enterprise Security Business Model (ESBM)™
  - SecurityATLAS ™
  - Managing IT as a Business
  - CIO Survey: The State of IT Security
  - Global Information Security Survey
- PwC maintains strong relationships with global financial regulators, financial industry groups such as BITS, Payment Card Industry Security Standards Council, and US law enforcement agencies such as the US Security Service, FBI, and DOJ.

Section 4 – How PwC can help
PwC's background (continued)

Analyst's view of PwC's security capabilities
• PwC was named a leader in the security consulting services market according to The Forrester Wave™: Security Consulting, Q1 2009 (March 2009). Forrester evaluated PwC's current offering and strategy for security consulting against approximately 80 criteria. Forrester's report states that "PwC has always led the way in developing and delivering the methodologies and practices that are consistent with the current market conditions."

Section 4 – How PwC can help

PwC can drive value by advising on the adoption of a strategic approach to security planning and assessment

- Help clients better align security governance and planning to support business objectives and compliance requirements.
- Increase the ease of funding for security projects from management by communicating information along multiple dimensions.
- Help develop, communicate and sustain a comprehensive security strategy that is actionable, repeatable, and reportable.
- Leverage PwC's SecurityATLAS tool set and overall security taxonomy, including various capability and process models to evaluate security programs.

PwC can help design, integrate, and implement technology architectures and security solutions

- Provide security architecture and design implementation services.
- Deliver application security as well as architecture and code reviews.
- Help design and implement identity and access management solutions.
- Design and implement integrated threat and vulnerability management solutions.
- Provide mobile security strategy, analysis, design, and assessment services.
- Help clients improve key security processes such as those supporting security communications and reporting.

PwC can help improve risk management and compliance activities

- Work with clients to identify risk areas and establish priorities for remediation.
- Use proven methodologies and deep industry knowledge to integrate security infrastructure (people, processes, and technology) and help implement standardized processes.
- Make it easier to monitor conformity with established standards and policies as well as maintain asset risk exposure within a known and accepted range.

Section 4 – How PwC can help

PwC can help manage the impact of a cyber attack
• Help companies respond to unplanned security events. • Provide security-related cyber crime dispute analysis and digital forensic services. • Help define security crisis and response policies and procedures. • Provide postmortem security services to analyze incidents and help prevent future occurrences. • Help define security monitoring processes and incident response policies and procedures.
PwC can help protect privacy
• Design and help implement privacy awareness programs. • Enhance reporting of privacy-related risks at the board, executive management, and task force level. • Perform integrated privacy and security assessments. • Inventory and map business processes that involve high-risk data elements throughout the data life cycle. • Help develop a third-party privacy and security oversight program with contractual safeguards, manual or automated precontract risk-based assessments, and ongoing auditing program.

Section 4 – How PwC can help

For further information, please contact:

John Garvey	john.garvey@us.pwc.com
	(646) 471-2422
Scott Evoy	scott.evoy@us.pwc.com
	(617) 530-7223
Andrew Toner	andrew.toner@us.pwc.com
	(646) 471-8327
Patrick Giacomini	patrick.a.giacomini@us.pwc.com
	(646) 471-4399
Sergio Pedro	sergio.m.pedro@us.pwc.com
	(646) 471-1928
Christopher Morris	christopher.morris@us.pwc.com
	(617) 530-7938

Section 5 – Select qualifications

Section 5 – Select qualifications

ATM breach response

Issue	The client was defrauded of millions of US dollars over a weekend via ATM machines around the world and suspected the fraud was related to a cyber breach. PwC was asked to provide advice and services to determine the root cause of the fraud.
Approach	PwC conducted key interviews and immediately began to forensically collect digital evidence and analyzed that evidence onsite. The investigation required multiple collaborative work streams with specific areas of focus. Specifically, there was a collaborative effort among crisis leadership, digital forensics, system-level and database analysis, augmentation of the client's SOC, enterprise data discovery, remediation of security weaknesses, and security enhancements in support of PCI standards. The analysis led to the identification of nearly 100 compromised systems, which were also collected, analyzed, and preserved as evidence. Ultimately, PwC forensically acquired over 200 systems totaling more than 30 terabytes of data and analyzed those systems. PwC located and analyzed more than 600 databases in the client's environment to support identity theft breach notification requirements. PwC's investigation discovered previously unknown malware. PwC's analysis of this malware to determine its functionality was not only key to preventing further attacks, but also useful to law enforcement and the technology industry.
Benefit	PwC's investigation determined that the incident involved more than substantial ATM card fraud, with millions of identities exposed. PwC was also able to consistently meet all client delivery requirements over the duration of the engagement. Further, PwC's investigation uncovered a previously unknown method to defraud ATM transactions, which benefited not only the client but also the entire financial industry. In support of legal counsel managing a variety of legal actions caused by the incident and resulting in a legal hold, PwC forensically preserved all electronic records of pertinent custodians.

Section 5 – Select qualifications

Financial institution sourcing challenges

Issue	The client wanted to reduce expenses and drive efficiencies through global business process outsourcing solutions. Its corporate operations and technology leadership recognized that privacy regulatory requirements and associated risks had not been evaluated by the business units. The leaders were concerned that cross-border data flows and initiatives involving potentially sensitive, personally identifiable information of customers and employees could be limited by privacy and data protection. In addition, the client recognized it lagged behind its peers and was not consistently addressing potentially significant risks because it lacked an enterprise-level governance approach.
Approach	PwC worked with the client to develop and execute a methodology, including an automated tool, to identify and classify the data elements that would flow across the globe and the countries where privacy regulatory requirements needed to be assessed. A risk control matrix was developed to consistently identify and present regulatory requirements and associated control objectives for privacy compliance in countries with overarching national privacy or data protection rules. Also a minimum requirements (leading practices) document was developed for use in countries without specific privacy regulatory requirements. Leveraging the PwC global network, the team worked with the client to risk-rate more than 100 countries and assessed them to determine the overall associated privacy risks. We also developed a privacy governance road map for the company focused on the key people, process, and technology components of an effective global compliance program, including an 18-month action plan, and worked with the client to help it execute the priorities.
Benefit	As a result of our work, our project sponsor was able to present to his internal business clients comprehensive privacy risk assessments and guidance on more than 30 priority right-placement initiatives and in-depth privacy risk assessments for the 100-plus countries involved. This work supported key business decisions central to the company's highly publicized efforts to reduce operating expenses and leverage operating efficiencies. We also helped the company develop its first global privacy governance approach and organization needed to manage privacy risks, which are increasingly the focus of attention that could otherwise negatively impact its trusted global brand.

Section 5 – Select qualifications

PCI remediation and payment switch system implementation

Issue	The client was accepting payment card transactions in a manner not compliant with the Payment Card Industry Data Security Standard. As such, it was facing fines if remediation efforts were not immediately taken. Complicating the client's remediation efforts was the existence of more than 25 identified applications that were accepting payment transactions across the enterprise. The disparate nature of the client's payment infrastructure made for a sizable project loaded with significant risks.
Approach	PwC presented a comprehensive solution that addressed not only the client's compliance burden, but also its disparate payment infrastructure. The firm leveraged resources from financial services and technology to develop implementation plans for a switch that would significantly shift the compliance burden away from a large number of applications to a centralized payment environment. Furthermore, for those applications not using the payment switch, our Advisory practice also led tactical remediation efforts to achieve compliance.
Benefit	The client realized several key benefits from this engagement. First, a smaller scope of compliance and better controls helped reduce resources and time necessary for annual audits. Next, by addressing the payment infrastructure, the client was better positioned to make enterprise-wide enhancements to its payment operations, as well as realize benefits within its treasury operations. The potential benefits for the client were in excess of $25 million over five years, plus significantly reduced compliance costs.

Section 5 – Select qualifications

Security framework design and implementation for service-oriented architecture for large investment management firm

Issue	The client wanted to standardize infrastructure and consolidate applications to take advantage of the latest Web services tools and techniques to provide real-time transactional services. The goal of this effort was to reduce varied, proprietary technologies and replace them with secure, open, standards-based technologies that enable collaboration among different business channels.
Approach	PwC designed and deployed a .Net based security infrastructure that included an access management product for Web services and a user directory infrastructure including a meta-directory using SAML standard for Web service security. We also designed and deployed role-based access control and user entitlements, integrated applications with the security framework services for single sign-on, and completed performance engineering for Web services security framework scalability.
Benefit	An open standards-based and secure wealth management platform translated into huge cost savings by: • Ease of integration with business partners • Enablement of outsourcing of distributed components and enforcement of service level agreements • Reduced sign on, rendering of business information from multiple applications under a common view • Reduced operational costs in the long term through aggregation of identity infrastructure components

Section 5 – Select qualifications
Security strategy for global card brand

Issue	The client was struggling with a disparate information technology landscape. These siloes created integration challenges resulting in higher costs and negative business impacts associated with an uncoordinated, unstructured IT security. In addition, the client was facing regulatory pressures around Sarbanes-Oxley and GLBA and needed a program to proactively manage these pressures. This well-known financial services institution recognized the advantages of developing a cohesive and actionable information security and data protection strategy.
Approach	PwC's approach to answering this challenge was to take a holistic view of the organization, considering people, process, and technology as intertwined rather than independent objectives: • People: Working closely with the Chief Information Security Officer (CISO) and his direct reports, PwC was asked to validate and, where appropriate, suggest improvements on the organization structure that was proposed for implementation in support of the CISO program office. • Process: Again, working in concert with the CISO and his direct reports, PwC assembled a set of program office activities. These activities defined the processes, metrics, and capabilities that should be considered and recognized by the organization where the goal is to manage security as a business. Furthermore, an analysis was conducted of activity hand-offs, overlaps, and gaps to suggest process improvements and allow the CISO to better understand the overall security landscape. • Technology: Over three-month period, PwC worked with various individuals in this organization to determine their current position and desired future state around a myriad of security disciplines. These disciplines covered security concerns that addressed both protection and enablement activities for the organization. The approach included an interview process that included representatives from a host of business units, security groups, and executive sponsorship. Furthermore, PwC leveraged our own industry knowledge and security experience to complete the strategy by supplying industry trends and best practices in the various areas. Lastly, we supplied a road map of interdependencies that assisted the organization in security investment activities and project portfolio management.
Benefit	This financial services organization, like most other organizations in this market, must be able to proactively respond to the multitude of demands shaping the face of information security today. Demands such as increased cyber threats and attacks, governance and compliance (such as SARBOX, GLBA, SB1386), increased threats and complex vulnerabilities, and customer and employee enablement (for example, identity management) are driving the need to develop a comprehensive enterprise security strategy. The development of this security strategy has enabled this financial services organization to understand how to respond to both external and internal demands. The security architecture road map being traversed by the organization fosters improved security investment allocation and project portfolio management. Having the information technology strategy, supporting processes, and organizational model in place promotes improved alignment with business objectives, decreases infrastructure redundancies, and improves operational effectiveness.

www.pwc.com