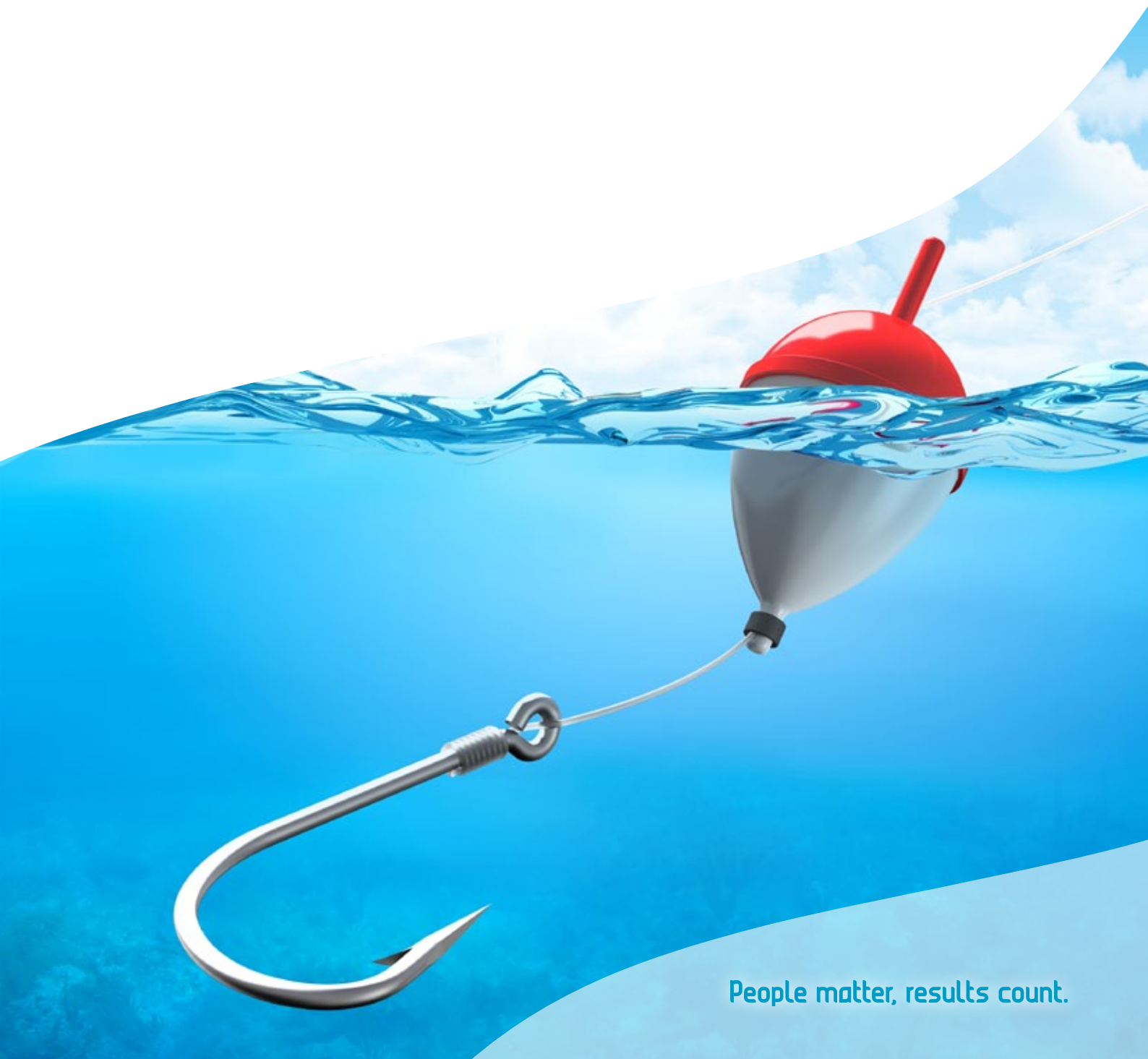
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Risk & Compliance | the way we see it

Data Privacy in the Financial Services Industry

How high-profile data breaches have impacted the privacy landscape



People matter, results count.

Contents

1 Overview

Divulging personally identifiable information during a business transaction has become a commonplace occurrence for most individuals. This activity can span from sharing of bank account numbers, loan account numbers, and credit/debit card numbers, to providing non-financial personally identifiable information such as name, social security number, driver's license number, address, and e-mail address. In short, there is a deluge of personally identifiable information that banking, capital markets, and insurance industries deal with and possess as a part of their day to day business.

Due to the rising threat of data breaches, identity theft, and associated fraud across industries, companies are increasingly focusing on enhancing data privacy programs. The problem of data breaches is a concern across all industries; however the financial services industry is a primary target of fraudsters due to the inherent value of the underlying data.

This paper discusses the importance of data privacy from the perspective of the financial services industry, with an emphasis on the challenges firms face in day-to-day business operations. It also analyzes the role that government organizations across the globe are playing in formulating privacy laws and overseeing compliance. Finally, we analyze the steps financial services firms need to take to better protect against data breach incidents through the design of proactive data privacy programs.

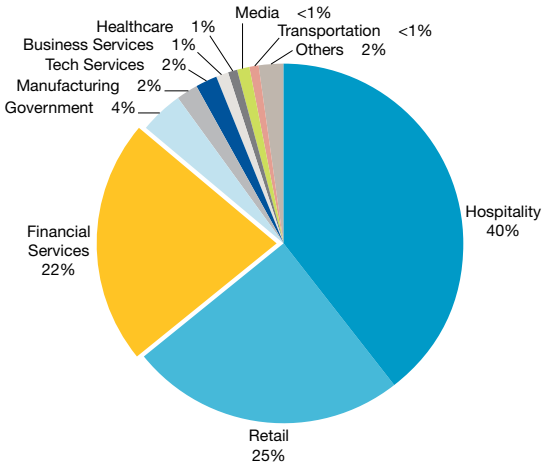
2 Data Privacy: An Industry Perspective

Maintaining the privacy of confidential customer information has become essential for any firm which collects or stores personally identifiable data. Such information may be general yet sensitive such as names, addresses, and social security numbers; or it can be crucial and financially sensitive data such as credit card, debit card or bank account numbers.

The financial services industry operates and deals with a significant amount of confidential client and customer data for daily business transactions. Due to the perceived value of this data, the financial services industry is one of the primary targets for data breaches.

As financial services institutions are the richest sources of personally identifiable information—both general and financial —they are primary breach targets and need a comprehensive data privacy strategy.

Exhibit 1: Industry Groups Represented by Breach Events (%), 2010



Source: Capgemini Analysis, 2011; 2011 Data Breach Investigations Report, Verizon

Hospitality, retail, and financial services have been among the industry verticals that were most affected by data breach events in 2010. Collectively these three verticals accounted for around 87% of data breach events recorded, with financial services accounting for almost 22% of total breach cases reported across industries in 2010[1]. On a positive note for the financial services industry, this 22% represents a drop from 33% in 2009. The 2010 drop is likely due to recent arrests and prosecutions following large scale intrusions in the financial services industry, which is also leading to increased focus on less reactive targets such as the retail and hospitality industries.

[1] 2011 Data Breach Investigations Report, Verizon

Another way to measure breaches is the number of records that were compromised. In 2010, approximately 35% of the total records compromised came from financial services. Even based on this measure, 2010 has been a relatively good year for the financial services industry since traditional historical average has been 90% or more. This decrease reflects the lack of large-scale mega breaches in the financial services space in 2010.

2.1. Data Privacy and its Importance in the Financial Services Industry

The financial services industry is one of the primary data breach targets due to the perceived value of the underlying data.

The operational structure of financial services institutions requires them to have more stringent data security standards as compared to those operating in other industries. On a regular basis, financial service firms deal with large amounts of personal and confidential customer information including bank account information, debit or credit card data and other business confidential customer data. Data privacy regulations and the potential reputational risks associated with breach events make having a strong data privacy policy in place even more important.

The success or failure of a financial service firm can depend on how it balances the use of confidential customer information while maintaining privacy. To capitalize on emerging growth opportunities, financial firms need to be flexible in sharing confidential customer data—whether across different departments, affiliated partners, or non-affiliated third parties such as technology or outsourcing firms—while complying with regulations and protecting the company's reputation. The key lies in this delicate balance between data sharing flexibility and maintaining data privacy.

3 Securing Data and Managing Breaches in the Financial Services Industry

3.1. A Look at High-Profile Data Breaches

A quick glance through some of the most high profile data breaches affecting U.S. customers highlights that six of the top ten data breach events that have occurred since 2007 were at financial service firms, though the number of breaches in the financial services firms has decreased in 2010 and 2011.

Six of the top ten data breach events that have occurred since 2007 were at financial service firms

Exhibit 2: Top Ten Data Breaches across Industries Affecting U.S. Consumers (2007-2011)

Date Reported	Breach event	Industry	Compromised Records (millions)
Jan 2009	**Heartland Payment Systems**	**Financial Services**	**130.0**
Jan 2007	TJ Stores (TJX)*	Retail/Merchant	100.0
Oct 2009	U.S. Military Veterans	Government	76.0
Aug 2008	**Countrywide Financial Corp.**	**Financial Services**	**17.0**
Mar 2008	**Bank of New York Mellon**	**Financial Services**	**12.5**
Apr 2011	Sony, PlayStation Network (PSN), Sony Online Entertainment (SOE)	Retail/Merchant	12.0
Jul 2007	**Fidelity National Information Services/ Certegy Check Services Inc.**	**Financial Services**	**8.5**
Jan 2009	**TD Ameritrade Holding Corp.**	**Financial Services**	**6.3**
Sep 2011	Tricare Management Activity, SAIC	Other	5.2
Jan 2009	**CheckFree Corp.**	**Financial Services**	**5.0**

* Includes TJMaxx, Marshalls and Winners in U.S., Puerto Rico, Canada, U.K. and Ireland
Source: Capgemini Analysis, 2011; Chronology of Data Breaches, www.privacyrights.org

While 2010 was relatively mild in terms of records breached, 2011 has been notable for a few high profile data breaches, notably the Sony PlayStation network breach which affected over 100 million customers globally. Additionally, the financial services industry witnessed data breaches involving large global firms such as Citigroup and Bank of America. In June 2011, Citigroup U.S. reported that hackers were able to gain unauthorized access to personally identifiable information such as customer names, account numbers, and contact information of around 360,000[2] customers . Citigroup Japan suffered a similar breach affecting around 92,400[3] customers . Bank of America suffered a massive insider breach in May 2011, which ended up costing the firm around US$10mn[4].

[2] Security breach: Citigroup says 360,000 accounts hacked, Hindustan Times, June 16, 2011
[3] Citigroup data breach hits 90,000 in Japan, Japan Today, August 6, 2011
[4] Insider data theft costs Bank of America $10 million, Computer World, May 25, 2011

These high profile corporate breaches have highlighted the difficulties faced by even the largest global businesses to consistently protect their digital assets. Despite having robust data privacy programs and data security systems in place, firms are still vulnerable to fraud through exploring loopholes in existing data protection systems and practices.

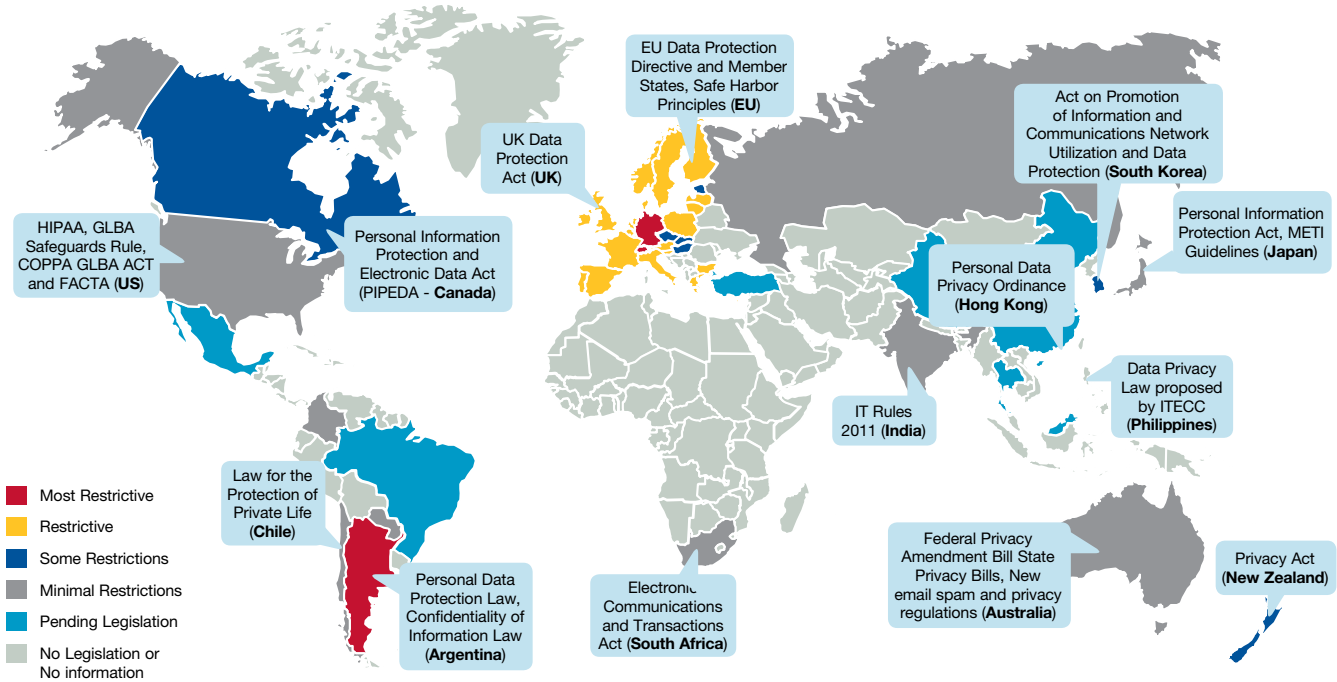
3.2. A Brief Overview of Privacy Regulations across the Globe

Maintaining privacy of data is a primary concerns for companies and governments across the globe. Most countries have privacy laws and regulations intended to protect personal and sensitive customer data from misuse. These laws set standards for companies in terms of how they use, store, and process such data. Countries such as the U.S. have passed regulations mandating the client notification of data breaches as soon as a breach occurs.

Data privacy laws are present in almost all major countries across the world. While they all revolve around data security, accountability, access, data integrity, consent, disclosure, and notice, the stringency levels of these laws and their enforcement differ.

The following exhibit categorizes major countries based on the level of stringency in their set privacy regulations and enforcement. Germany and Argentina have the most restrictive laws and strictly prohibit data transfers to countries without adequate data protection regulations. Most other Western European countries fall in the restrictive category.

Exhibit 3: Guide to Region and Country Specific Regulations



Note: Country boundaries on diagram are approximate and representative only.
Source: Capgemini Analysis, 2011; Forrester Research, 2010; International Privacy Laws

Undoubtedly, the changing technological landscape has had a major role to play in the rapidly evolving privacy environment. Various countries that have relatively weaker privacy legislation are now updating their privacy laws to be better positioned for the technological advancements.

The essence of the evolving privacy laws is on the protection and maintenance of customer's personal information. However, the stringent nature of these privacy laws and regulations can pose business challenges for firms that have centralized operations with a presence in multiple locations as well as firms that work with external vendors in offshore locations. For example, the European Union data protection directive imposes restrictions on the transfer of all personal information outside the EU region. The U.S. on the other hand has no specific laws addressing cross-border flow of data but has various laws which require firms to secure all personally identifiable information.

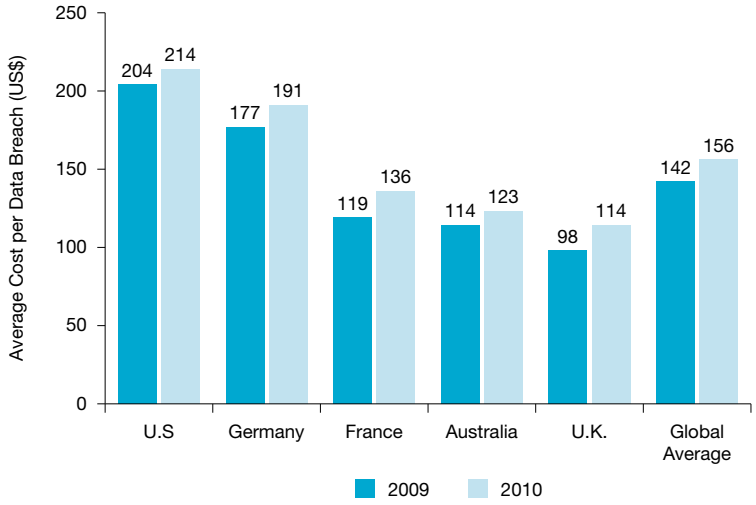
> "The ability of bad guys to enter, steal, exit and do it in a way that's undetectable is rising…"
>
> **Larry Ponemon**
> June 2011

The challenges posed by disparities in market-specific privacy laws standards have been addressed relatively well, with most governments focusing on the harmonization of privacy laws. India, one of the leading outsourcing service providers to many mature markets, has recently developed a comprehensive set of data privacy rules under new legislation. This legislation, termed the Information Technology Rules 2011, applies to all companies including back office and third party outsourcing firms in order to strengthen data privacy laws in the country. Mexico, another upcoming outsourcing destination, joined 50 other countries in adopting broad privacy regulations focusing on private sector firms.

3.3. Cost Implications of Data Breaches

Data breaches have become an uncomfortably common feature in today's business context and quite often make news headlines. The cost of a data attack for any company can be huge and has been increasing in recent years.

Exhibit 4: Average Data Breach Costs per Record (US$) 2009–2010



Source: Capgemini Analysis, 2011; 2011 Data Breach Investigations Report, Verizon

Malicious or criminal attacks, third-party mistakes, and loss or theft of data storage devices like laptops have led to an increased average cost of data breaches in 2010.

In 2010, the average cost of data breach has increased across the globe[5] with the U.S. breaches costing around US$214 per record compromised[6], and a global average of US$156.

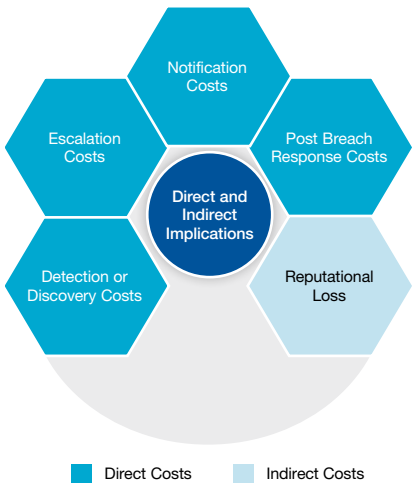
In fact, data breach costs have shown an increasing trend over the past four years. Malicious/criminal attacks, third-party mistakes, and loss or theft of data storage devices (such as laptops) have led to an increased average cost of data breaches in 2010. The increase has been especially true for firms that have shown an inability to prevent and counter these threats. Additionally, the lack of proper breach response plans by firms has also been a key driver of rising data breach costs.

An analysis of the costs incurred in 2010 reveal that reputational losses, as well as post-breach response costs, is increasingly becoming one of the primary components of overall data breach costs outside of the U.S. In the U.S., regulatory compliance is the main driver of data breach mitigation costs.

Firms that are subjected to a data breach bear both direct and indirect costs. Breach detection and escalation costs; costs of notifying affected customers; and other response costs such as setting up a communication platform to help breach victims are direct costs that can be measured by the labor and money spent on these activities. Additionally, firms that are found to have been guilty of breach due to non-compliance of existing privacy laws and weak data security policies may have to incur other costs in the form of legal fines.

However, there are also indirect costs such as reputational costs which can only be measured on an economic estimate of lost business opportunities.

Exhibit 5: Cost Implications of Data Breach for Financial Services Industry



Source: Capgemini Analysis, 2011; Annual Study: Global Cost of Data Breach, Ponemon Institute and Symantec, May 2011

[5] 2010 Annual Study: Global Cost of a Data Breach, Ponemon Institute, Symantec
[6] Average cost of data breach per person affected

Despite the availability of automated data loss prevention solutions, employees still play an integral part in avoiding data leaks and handling sensitive data.

3.4. Challenges to Data Breach Prevention in an Organizational Setup

Due to increasing scrutiny from regulators and the media, financial services institutions continue to face pressure to maintain high standards of data security.

Today, financial firms face the following challenges when addressing privacy concerns and regulations.

- **Information flexibility.** Financial service institutions need to provide dynamic access to sensitive customer data to clients, employees, and external partners. Such a high flow of information exchange can make it difficult to protect data.
- **Proliferation of social media.** Social networking sites are being used extensively for purposes such as brand building and establishing relationships with customers. While social media provides a relatively inexpensive method of marketing financial products/services and better connecting with the customers, it also provides challenges in maintaining data security.
- **Sophisticated external hackers.** Cyber criminals are increasingly using sophisticated viruses, malware, and other techniques designed to outsmart traditional data security technologies.
- **Educating employees in data protection.** Despite firms having automated data loss prevention (DLP) solutions, employees still play an integral part in avoiding data leaks and handling sensitive data. As a result, it can be a challenge to continually educate both new and existing staff about various security issues.

4 Emerging Global Data Privacy Trends

Evolving data breach threats are forcing sweeping regulatory changes. With the help of technology, financial service institutions are developing and implementing operational and procedural changes in order to comply. The framework below captures certain emerging trends in three areas witnessed in the wake of data breaches: Data Breach Evolution, Regulatory Focus, and Technology.

Exhibit 6: Emerging Data Privacy Trends

Data Breach Evolution	Regulatory	Technology Adoption
▪ Growing data breach risks and malicious insiders ▪ Growing threat of financial malwares to financial firms ▪ Increasing data breach mistakes	▪ Increasing government focus on law enforcement and breach notification ▪ Harmonization of data protection standards across regions ▪ Outsourcing destinations adapting privacy laws to help industry	▪ Increasing use of identity and access management solutions ▪ Focus on simplifying data protection and controlling costs ▪ Using smartphones to provide cyber security

Source: Capgemini Analysis, 2011

4.1. Data Breach Evolution

Financial service firms are now facing data breach risks not just from internal and external attacks, but also from unintentional mistakes.

The economic downturn led to employee layoffs over the past two or three years resulting in an increasing number of disgruntled employees, who in turn are susceptible to stealing or disclosing customer information.

Growing data breach risks from malicious insiders

The percentage of data breaches attributable to insiders more than doubled to 46% in 2010[7]. The economic downturn led to employee layoffs over the past two or three years resulting in an increasing number of disgruntled employees, who in turn are susceptible to stealing or disclosing customer information. In most cases, intentional insider breaches have the potential to cause greater financial losses to a firm than an outside attack as insiders generally tend to have full knowledge about where important and sensitive data is stored.

Growing threat of financial malwares

Malware, or malicious programs designed with the intention of stealing financial data, have grown rapidly to become a leading cause of breach, especially for smaller financial firms. Malware aids cyber criminals who use it to efficiently gather sensitive information through the internet.

[7] 2010 Data Breach Investigations Report, Verizon

The Zeus platform-based Ramnit virus has been one of the recent worms affecting financial firms' data security. OddJob, another relatively recent malware, has the ability to hijack customer online banking sessions in real-time by using the customer's session ID tokens. Such new malware highlights the fact that hackers are getting inventive in breaching financial data. In addition, this malware allows hackers to sit at one country and execute fraudulent transactions across the globe. For instance the OddJob malware has been used extensively in Eastern Europe to attack banking customers in various countries including the U.S.

The risks of unintentional data breaches due to unforeseen problems such as lost laptops or improper data disposal remain quite high.

Increasing data breach mistakes

While the possibility of a data breach from internal and external malicious attacks is often discussed, the risks of unintentional data breaches due to unforeseen problems such as lost laptops or improper data disposal remain quite high and can have a significant impact on a company. The challenge that most firms face is that people still do not fully understand the need to safeguard data and the efforts by firms to train employees do not seem to have yet provided the desired results. Firms are expected to continue investing time and resources in order to ensure that what is meant to stay confidential does stay confidential.

4.2. Regulatory Focus

Globally, legislation is increasingly focusing on enacting laws that maximize data privacy and minimize breach impact on businesses.

Increasing government focus on law enforcement and breach notification

Regulators across the world are seeking stricter law enforcement through tougher penalties on data breach violators. In the European Union, data protection authorities can now investigate and prosecute organizations for non-compliance. Several other countries are intensifying their existing law enforcement policies. While the U.S. has been one of the earliest to adopt breach notification requirements, other nations are following suit.

Harmonization of data protection standards across regions

Data protection standards vary across the world with no unified approach, which comes at a cost—especially for banks, insurers and capital markets firms which have multinational operations and deal with third party vendors such as offshore outsourcing partners and local governing bodies. The European commission has recently vowed to resolve this issue by cutting down excessively bureaucratic and ineffective notification requirements across the region. The European commission also plans to establish a voluntary registry for companies in non-EU countries that agree to abide by the EU data security standards, in a bid to simplify data security. In order to comply with the stringent data security standards set by the EU's Data Protection Directive, many emerging countries are beginning to adopt these broad privacy regulations.

To comply with the stringent data security standards set by the European Union's Data Protection Directive, many emerging countries are beginning to adopt these broad privacy regulations.

Outsourcing destinations adapting privacy laws to help industry
To enhance data security standards and alleviate privacy concerns around foreign countries, most outsourcing destination countries—including India—have recently implemented new data privacy rules. Originally, proposed privacy regulations set by India required firms to obtain the consent of end customers before it could collect their personal information. Such regulations, if implemented, would have posed a new set of challenges to the outsourcing business. The Indian government later clarified that they have exempted outsourcing companies from these regulations in India, a move that is expected to minimize any negative effects of the latest privacy regulations on the outsourcing industry.

4.3. Technological Evolution

Firms are using technology to enhance data protection and better control compliance-related costs.

Increasing use of identity and access management solutions
The financial service industry is increasingly investing in identity management and control tools to limit access to critical information and keep track of who has access to what information. Identity and access management tools, which traditionally performed the function of a gatekeeper, have evolved with technology and are now being used to perform advanced functions such as: defining access levels; tracking of events with regards to when a particular breach has taken place; locating where the breach happened; and identifying the time of the breach occurrence.

Focus on simplifying data protection and controlling costs
Driven by the advent of new computing models, the deluge of backup applications, and the multitude of network choices, the complexity of data protection has increased for all organizations. Security officers are expected to look for storage pooling in order to meet various data protection requirements, including but not limited to classifying data and policy management.

Using smartphones to provide cyber security
Major banks such as Citibank, Bank of America, and Chase currently send texts to customers on their mobile phones to alert them about large purchases or unusual account activity. Banks are now looking to convert their customers' smartphones into security tokens in order to provide them with an additional layer of protection, especially for online transactions. To convert these smartphones into security tokens, banks just need to install software that will enable these smartphones to generate new passwords frequently, saving the cost of providing customers with a separate security key fob.

5 Data Privacy Recommendations and Solutions for Financial Services Institutions

Securing data in the current information age is one of the biggest challenges faced by firms. Various data breaches reported by companies in the recent past highlight that a data breach can take multiple forms and that there is no single solution to stop these breaches. Data breaches can be caused by variety of reasons, ranging from an improper data disposal processes to weak data security practices.

Financial service firms need to be flexible in using and sharing non-public confidential customer data, which makes them vulnerable to data breach risks at various stages of their business process.

A comprehensive data privacy program is essential in an organizational setup due to the omnipresent nature of the data breach risks. The essence of a data privacy program is risk reduction through a well-planned and properly implemented privacy policy. We have detailed a few steps to effectively implement a comprehensive data privacy program in an organizational setup:

1. Identifying and classifying sensitive information
2. Scaling down the accessibility of information through data monitoring as well as identity and access management solutions
3. Safeguarding information through a variety of data security controls and advanced technologies such as encryption, tokenization, and data masking
4. Having a clear data disposal policy in place
5. Planning for a security breach by having a contingency breach response plan

The recent spate of data breaches have highlighted that breaches are ubiquitous, however organizations need to understand that both internal and external breaches can be preventable. Listed below are recommendations for financial services firms to enhance data privacy for their digital assets.

- **Centrally manage endpoint solutions.** Firms can lower or stop external incursion by better managing endpoint solutions for security patch deployment, information access, and encryption capabilities.
- **Align global security with real-time threat alerts.** Use a security information and event management system that can identify known threats and problematic sites and block them immediately.
- **Proactively protect data.** Implement a unified data protection policy including individual systems, servers, networks, and endpoints which, with the aid of appropriate DLP solutions, can also stop data extraction in case of an external breach.
- **Implement automated compliance controls.** Ensure that IT compliance controls conform to industry standards such as Payment Card Industry Data Security Standards and the Gramm-Leach Bliley Act and ensure maximum data protection.
- **Integrate security solutions with regular operations.** Create an operational model that is content-wise, workflow-driven, and can identify as well as cement any gaps in the security process.

The cost of a data breach usually far exceeds the investments in such proactive protection steps.

7 Conclusion

Financial service institutions have traditionally considered data privacy as a compliance cost. However going beyond compliance costs, reputational damages due to data breaches that expose confidential customer information can cost firms significantly. It is therefore imperative for financial services firms to have a comprehensive data privacy program with a combination of policies, access controls, and various DLP technologies that enable them to continuously protect themselves against emerging threats. While a strong data security management is crucial in the current business landscape, failures are unavoidable. Therefore, firms also need to have a breach response plan in order to prepare for a breach contingency. Having contingency plans as well as a proactive data privacy policy, are of key importance for all organizations.

The cost implications of a data breach from both monetary and reputational perspective are increasing exponentially for financial firms. Accordingly, the risk management team of every financial service institute needs to play an active role in shaping policies regarding data security, in close partnership with their firms' information technology groups.

Appendix A: Managing Data Privacy in a Cloud Environment

Privacy Landscape in a Cloud Environment

Though the financial services industry has generally been an early adopter of new technologies, the industry has been slow in embracing cloud technology due to privacy concerns. Compliance to stringent regulations is one of the primary reasons why the financial service industry has been skeptical about adopting public cloud services. Financial institutions are expected to better leverage public cloud-based platforms in the future as the security concerns around these platforms are properly addressed.

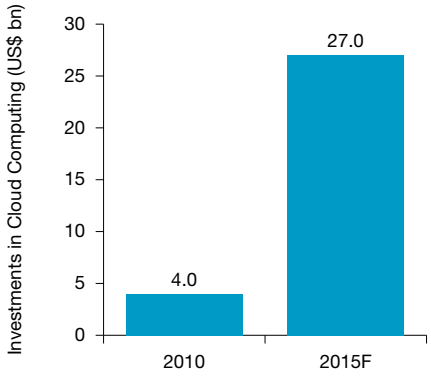
In the meanwhile, firms are expected to use a hybrid cloud platform which is arguably more secure and can address some of the compliance related restrictions. At the same time, hybrid cloud platforms also help firms reduce operational costs due to the pay-as-you-go capacity model that cloud services provide compared to traditional in house models.

Moreover, financial service companies that are contemplating cloud adoption are expected to go for a staged approach by moving basic low risk services such as email, collaborative software and testing and development as a first step to virtualization. As the benefits of cloud adoption evolve, firms can slowly move their business intelligence and other back office support applications before moving legacy applications such as policy administration and underwriting for insurers.

Cloud Adoption in the Financial Services Industry

On June 1, 2011, NYSE Technologies—the commercial technology division of NYSE Euronext—launched a first-of-its-kind completely cloud-based capital markets community. NYSE's stated reason for moving to a cloud environment is to create a virtual community for the capital markets with rapid access to global markets and actionable market information.

Exhibit 7: Investments in Cloud Computing by Financial Services Industry (US$ bn) (2010–2015F)



Source: Capgemini Analysis, 2011 and *Destination 2015: Spending on Cloud Computing in Financial Services* by Rodney Nelsestuen , June 20, 2011, Tower Group

Investments in cloud computing by the financial services industry are expected to grow phenomenally over the next few years as security fears are alleviated to reach US$27.0 bn by 2015, from an estimated US$4.0 bn in 2010.

The high cost of the traditional IT delivery model as compared to the cloud-based model, as well as the variable nature of certain IT services which can be flexibility managed through cloud, is expected to drive cloud based services. Smaller firms such as small regional banks are expected to take a lead in cloud adoption in order to "do more with less" as they are limited not just with technology budgets but also with staff.

However, it is noteworthy that despite the rapid 35% CAGR growth expected in cloud-based service usage during the 2010 to 2015 period, cloud-based services would represent only about 6% of the IT spending by 2015 for the financial services industry.

Appendix B: Managing Data Privacy in an Offshore Environment

Drivers and Challenges for Outsourcing to Offshore Locations

Over the past decades, many banks, insurers and capital markets firms have outsourced their back office and information technology operations to low cost destinations such as India, China and Malaysia to rationalize costs and operations. While cost advantage is a major driver for financial services institutions to outsource—whether to a third party vendor or a captive center—the perceived privacy risks can sometimes act as a major deterrent.

The basic rule in an outsourcing arrangement as per various privacy acts is that the responsibility for compliance lies with the company and not the outsourcing vendor.

In many countries including the U.S., high domestic unemployment rates have made outsourcing a political issue. Hikes in visa fees and the state of Ohio's ban on outsourcing IT services to foreign countries are examples of anti-outsourcing sentiment in the U.S. This highlights some of the challenges that firms face at the state level which can be further complicated in case of a breach event in an offshore location. The increased regulatory scrutiny and strong opposition by certain governments against outsourcing adds further pressure on financial service institutions to counter data privacy in an offshore setup. Further, media hype has also focused in on data security concerns for outsourcing despite the vested economic benefits.

Essential Preconditions for a Successful Outsourcing Relationship

Financial services institutions thinking of outsourcing any of their operations or processes to a third party vendor in an offshore location need to consider the limitations they may face due to the privacy laws in the source country as well as the destination country. One of the essential pre-conditions in the vendor qualification process needs to be the ability of the vendor to fulfill the company's privacy obligation under its own country's laws as well as the country from where data is being sourced.

Before deciding on an outsourcing partner, financial services institutions should consider vendor practices that impact privacy such as human resource practices, operational processes, infrastructure setup, and the policy framework:

- **Human Resource practices.** Firms should ensure that outsourcing vendors follow best practices in human resources such as performing suitable background checks and screening employees. Additionally, entering into a non-disclosure agreement with the outsourcing vendor also goes a long way in maintaining high privacy standards.
- **Operational procedures.** Firms must ensure that the vendor's operational system is as good as their own through implementation of data security solutions. To plan for contingent events, outsourcing vendors should also have a robust business continuity plan along with a system for conducting periodic audits.
- **Infrastructure setup.** Firms should check that the infrastructure setup of an outsourcing vendor has the required security infrastructure in the form of a robust network security system with firewalls and endpoint protection to tackle online issues. Additionally, having physical access to controls and restrictions can help in reducing any issues of unauthorized access which can lead to breach threats.
- **Policy framework.** Firms need to ensure that the outsourcing vendor has stringent security policies which are embedded in the organizational culture and are part of routine operations. Non-adherence to established security standards should be strictly penalized.

Additionally, outsourcers can allay the security concerns of financial services firms by arranging for independent security and privacy assessments from notable third party organizations. Certifications like SAS 70 can demonstrate offshore vendors have adequate controls and safeguards when they host or process data.

References

1. *Data Loss Prevention: Data-at-Rest vs. Data-in-Motion*, www.identityfinder.com accessed July 2011

2. *2010 Annual Study: Global Cost of a Data Breach*, Ponemon Institute and Symantec, May 2011

3. *Cashing in on Banking Security and Compliance*, Ipswitch, May 2010

4. *Chronology of Data Breach*; www.privacyrights.org accessed October 2011

5. *Interactive Data Protection Heat Map*, Forrester Research, 2010

6. *Financial Malware Hijacks Online Banking Sessions*, www.net-security.org, February 2011

7. *Ramnit Virus Targets Banks*, www.banktech.com, August 2011

8. *Data breach mistakes feared more than attackers*, www.net-security.org, April 2011

9. *European Commission Vows to Simplify Data Protection*, CIO, May 2011

10. *India Exempts Outsourcers From New Privacy Rules*, www.csoonline.com, August 2011

11. *Firms enlist smartphones to provide cyber security*, Boston Globe, August 2011

12. *3 Top Trends in Data Protection for 2011*, Enterprise Systems, January 2011

13. *Destination 2015: Spending on Cloud Computing in Financial Services* by Rodney Nelsestuen , June 20, 2011, Tower Group

14. *Outsourcers look to data security transparency for competitive advantage*, www.computerweekly.com, July 2011

15. *Anatomy of Data Breach – Why Breaches Happen and What to Do About It*, Symantec 2009

16. *A New Urgency in Data Protection*, www.banktech.com, accessed October 2011

About the Author

Santosh Ejanthkar is a Lead Consultant in Capgemini's Strategic Analysis Group within the Global Financial Services Market Intelligence team. He has over seven years of experience in research and strategy consulting for investment banking, asset management, private banking, and wealth management businesses.

The author would like to thank **Ramaswamy Vaidyanath, William Sullivan** and **David Wilson** for their overall contribution on this publication.

For more information, visit **www.capgemini.com/risk** or e-mail **riskmgmt@capgemini.com.**

About Capgemini and the Collaborative Business Experience

Capgemini, one of the world's foremost providers of consulting, technology and outsourcing services, enables its clients to transform and perform through technologies.

Capgemini provides its clients with insights and capabilities that boost their freedom to achieve superior results through a unique way of working, the Collaborative Business Experience™.

The Group relies on its global delivery model called Rightshore®, which aims to get the right balance of the best talent from multiple locations, working as one team to create and deliver the optimum solution for clients.

Present in 40 countries, Capgemini reported 2010 global revenues of EUR 8.7 billion and employs around 112,000 people worldwide.

Capgemini's Global Financial Services Business Unit brings deep industry experience, innovative service offerings and next generation global delivery to serve the financial services industry.

With a network of 21,000 professionals serving over 900 clients worldwide, Capgemini collaborates with leading banks, insurers and capital market companies to deliver business and IT solutions and thought leadership which create tangible value.

For more information please visit **www.capgemini.com/financialservices**