Financial institutions likely to remain top cybercrime target

Protecting assets and reputation through a **sustainable security infrastructure**

Confidence in a connected world. Symantec™

Contents

Introduction

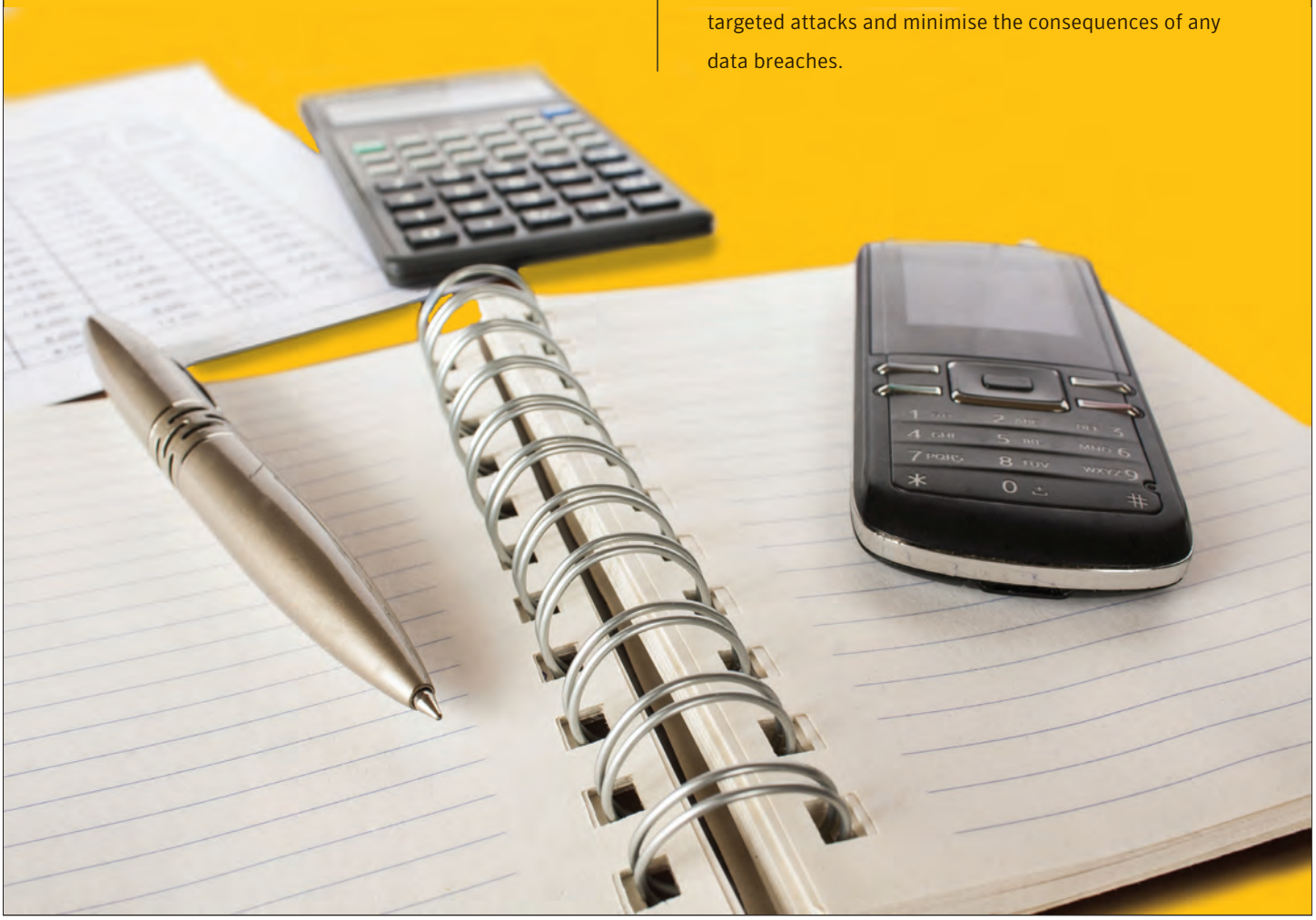
Attacks against the finance industry are becoming increasingly sophisticated and highly targeted.

Historically, a common (and highly successful) method of targeting banks has been to direct email phishing at customers. Now, emerging channels, such as mobile and online banking, are opening new doors for cybercriminals. To decrease the effectiveness of such attacks, banks have improved both communications to, and the education of, customers, as well as rapidly reacting if an attack occurs. However, criminals have responded not only by creating specialised malicious software designed to compromise online bank accounts, but also by subverting the servers and software owned by reputable institutions to improve the effectiveness of their phishing campaigns; a technique known as infrastructure hijacking.

According to the FBI, the latest trend by cybercriminals is to gain employee login credentials by using spam and phishing emails, keystroke loggers and remote access trojans. Such attacks were seen in September 2012, when the Bank of America and Wells Fargo were among those struck[1].

The Financial Services Information Sharing and Analysis Centre has raised the threat level for attacks from 'elevated' to 'high', citing "recent credible intelligence regarding the potential" for distributed denial-of-service (DDoS) attacks[2].

This report contains recommendations and best practices to help organisations develop a sustainable security infrastructure designed to respond quickly to targeted attacks and minimise the consequences of any data breaches.



Meeting the challenge of targeted attacks

Mass-market attacks against all industry sectors remain common, but these are believed to be relatively unsuccessful within the finance industry. In general, and in comparison with other industries, the finance industry has a superior level of protection against malware and the running of unauthorised software on endpoints. However, the most dangerous threats are from well-resourced, sophisticated attackers who will research and craft a specific, targeted attack against a financial institution in anticipation of rich rewards if successful.

Whilst a DDoS attack is worrying, bringing down a website does not bring down the system. The financial industry, with its high standards in security and availability, is generally able to resist these attacks. Successful DDoS attacks may be highly visible and cause embarrassment for the affected institution, but they are unlikely to result in large financial losses. However, they should not be underestimated as they can serve as a distraction to leverage other attacks that then pass unnoticed.

The majority of targeted attacks against the finance industry are likely to be for financial gain. For example, over 300,000 online Citibank accounts were compromised in a targeted hack of the organisation's network in 2011[3]. The size of losses from such attacks is rarely disclosed by businesses, however, according to a 2011 Symantec State of Security survey, some 20% of large enterprise companies quoted an average of $195,000 in estimated damages[4].

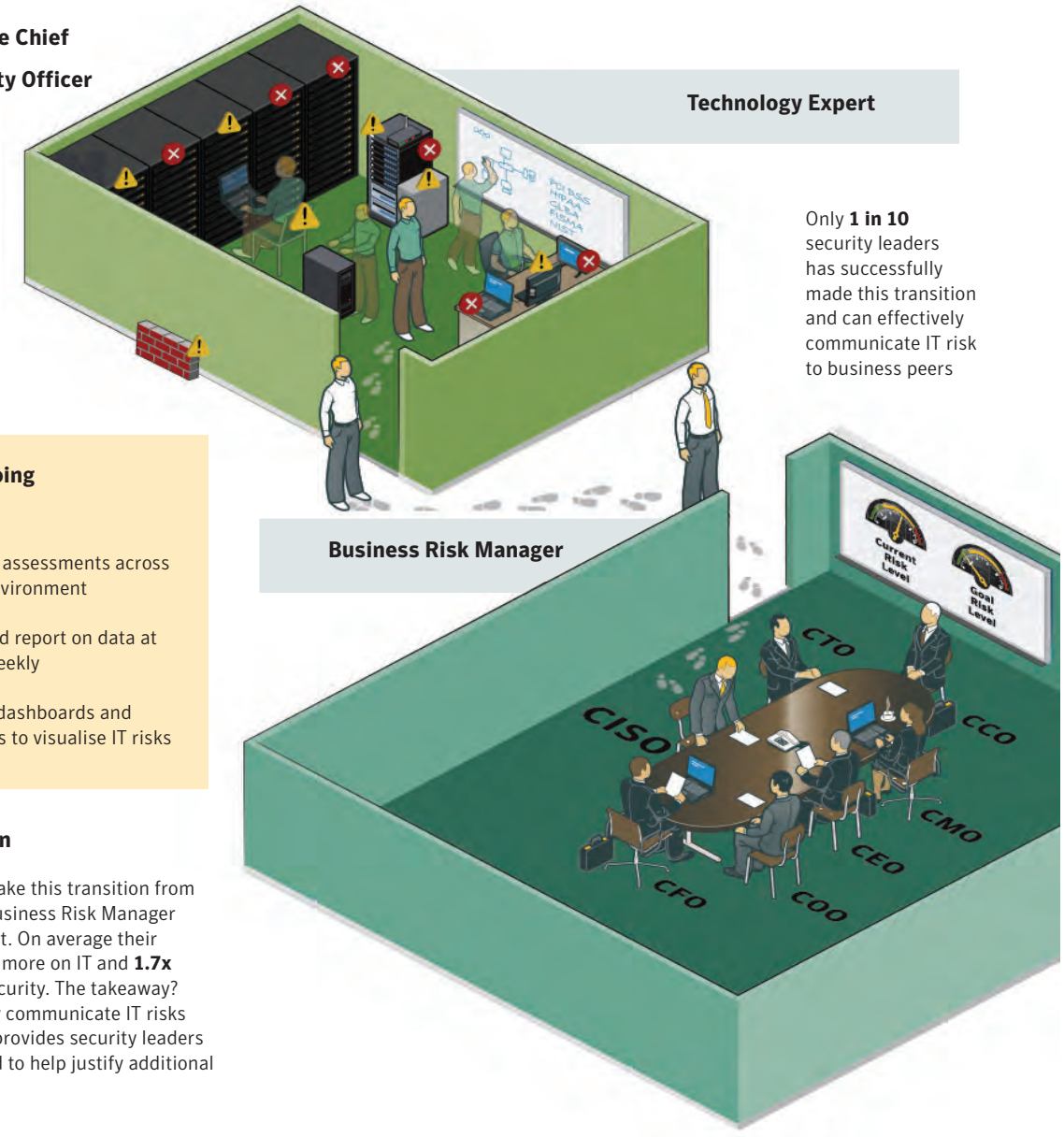
According to the Symantec Internet Security Threat Report, targeted attacks use customised malware and refined social engineering to gain unauthorised access to sensitive information[5]. Such attacks, where malware is sent by email, have increased from an average of 77 per day in 2010 to 82 per day in 2011. Symantec has also identified a new trend in these attacks.
The threat report data demonstrates that these threats are not limited to enterprise-sized organisations. Approximately 50% of attacks focused on companies with less than 2,500 employees, and another 18% focused on organisations with less than 250 employees. So, it appears no organisation is too small to escape the attention of attackers. In some instances, it may not be the organisation itself that is the ultimate target but, once compromised, it can be used as a staging point to increase the success of an attack against a subsequent target.

While the September 2012 cyber attacks mentioned in the introduction to this report only affected a few organisations, the potential for widespread global impact is real. Whether the motivation is obtaining confidential information, financial gain, or simply 'hacktivism', disrupting the financial services industry has the potential to disrupt the global economy. For this reason, information protection is no longer an IT-only conversation within an organisation. C-level executives, board members and even governments are now more concerned than ever with protecting information and keeping both businesses and the critical national infrastructure up and running.

A balancing act

Security is no longer a one-size-fits-all solution. Instead, companies must take a holistic approach to creating programmes that work. Technologies evolve and new threats and vulnerabilities emerge. As such, the role of the CISO is changing. Information security is not a final destination, but a journey in which the CISO must align closely with the business to ensure operational competitiveness and growth.

Changing role of the Chief Information Security Officer



Only **1 in 10** security leaders has successfully made this transition and can effectively communicate IT risk to business peers

What are they doing differently?

69% Automate assessments across their IT environment

61% Collect and report on data at least bi-weekly

75% Leverage dashboards and scorecards to visualise IT risks

A valuable transition

Security leaders who make this transition from Technology Expert to Business Risk Manager also secure more budget. On average their organisations spend **3x** more on IT and **1.7x** more on information security. The takeaway? Being able to effectively communicate IT risks in business terms also provides security leaders with the metrics needed to help justify additional security investments.

Figure 1: The changing role of the CISO (Source: IT Policy Compliance Group, Data Driven Reporting and Communications about IT: Better Results, Less Risk, February 2012)

Risk versus opportunity

The financial services industry needs to balance the protection of the banks' information and assets against the needs of employees, partners and customers to access information at preferred times and locations.

Banks have to innovate to be competitive and expose themselves to risk, without jeopardising reputation and financial assets.

Social media is an emerging customer channel, a point of contact and a potential point of sale. Nearly 75% of banking employees are making use of social media, yet only 20% of banks have deployed technical controls to block or limit organisational usage[6]. This opens up a new window of opportunity for criminals to use social engineering to target victims or spread infected links.

Mobile devices offer productivity gains and improve the quality of services delivered to customers and partners. However, they also increase exposure to risk. Although malware is not prevalent, the risk comes from phishing and fraud through unprotected mobile devices. In fact, mobile computing was identified as a primary risk in a Symantec report released in February 2012[7]. In addition, the frequently used out-of-band authentication through mobile devices, where the mobile is used to add multi-factor authentication, could emerge as a target for attacks if adoption increases. Mobile banking, payments, services and employee mobility represent the major risks for a financial institution as the Symantec report "Harnessing the Potential of Mobile and Banking" explains[8].

Cloud enables IT departments to distribute costs, deliver new services more rapidly, scale capacity and outsource applications and systems. However, it also brings potential risks. Transactional data and customer information need to be protected according to regulations and policies, and the security officer needs to understand potential exposure to cyber-attacks. Much of the finance industry has already implemented or purchased cloud computing services, and there is a consensus that the benefits outweigh the security risks. Nevertheless, cloud services must be integrated into the overall security infrastructure.

Security versus cost

Strategies to manage risk within the financial services industry typically include:

- Transferring risk to another party
- Avoiding risk
- Reducing the negative effect or probability of risk
- Accepting some, or all, of the potential or actual consequences of a particular risk

These strategies should be considered alongside related costs and available budget.

IDC has predicted that 15% of the IT budget in 2012 would be for risk management in the financial services industry[9]. According to a 2012 Deloitte survey, more than 70% of banking respondents dedicate at least 1-3% of their IT budget to information security, but the lack of sufficient budget and/or resources was also cited as the top barrier for an effective information security programme[10].

Regulatory pressure versus actual risk

As regulatory pressure increases, the finance industry needs to comply, but there is a risk that this can divert focus from targeted attacks.

The information security programmes of the financial services industry are generally of a high standard. However, excessive access rights, security policies and standards that have not been operationalised, alongside a lack of sufficient segregation of duties, can increase the risk of attack. Companies must ensure that regulatory compliance does not come at the price of protecting against targeted attacks that could impact upon reputation and customer loyalty, not to mention inflicting major financial loss.

Threat intelligence is essential

The way to stay ahead is to have access to the right intelligence and the knowledge to make use of it. As technology evolves and user behaviours change, any security intelligence needs to proactively seek to understand future threats.

Understanding targets and motivations

Banks are as exposed to 'mass market' attacks as any other organisation. But the greatest threat is probably from targeted attacks as these can be more difficult to detect and the attacker may focus on a specific system or set of information. Attackers generally fall into three broad categories:

- The financially motivated attacker who intends to compromise systems to conduct theft or fraud electronically.
- The espionage motivated attacker who intends to steal information to sell on to a third party.
- The politically motivated attacker who intends to compromise information or systems to achieve a goal shared within a group.

Banks should expect to be exposed to attacks from individuals or groups with all of these motivations. When Symantec measured the strength of association between industry SIC code and email targeted attacks, a strong association was found between the financial sector and targeted attacks. Indeed, credit unions and state commercial banks appeared to be at the highest risk of attack within all the industry groups studied[11].

The implications are that the banking and financial sectors are at high risk of targeted attacks that span the domains of IT security, fraud prevention and detection, and information privacy. However, such attacks can be defended against if organisations implement a multi-layer approach to security: making it as difficult as possible for attackers to compromise systems and maximising the speed of attack detection.

Breaches and identity theft are evolving

In a recent analysis of data breach trends in 2012, Symantec's Norton Cybercrime Index (CCI) found that while the number of breaches is fairly consistent with 2011, the average number of identities stolen has halved[12].

One reason for this could be that following a number of large high-profile breaches in 2011, many enterprises have taken steps to shelter customer record databases from Internet attacks. However, it could also be because hackers aren't pursuing large data breaches, targeting instead smaller breaches that contain more sensitive information.

In addition, although the numbers of breaches in 2012 are down compared to 2011, they do appear to be on an upward trajectory.

We know that not all data breaches are the result of cybercrime. Stolen mobile devices, lost hardware and website coding mistakes can all accidentally expose private data to the public. However, the Symantec CCI Index found that 88% of all identities stolen in data breaches during 2012 were the result of hacking. The trend was also seen in the end of 2011 data set, with the number rising from 14% in May up to 74% in December 2011.

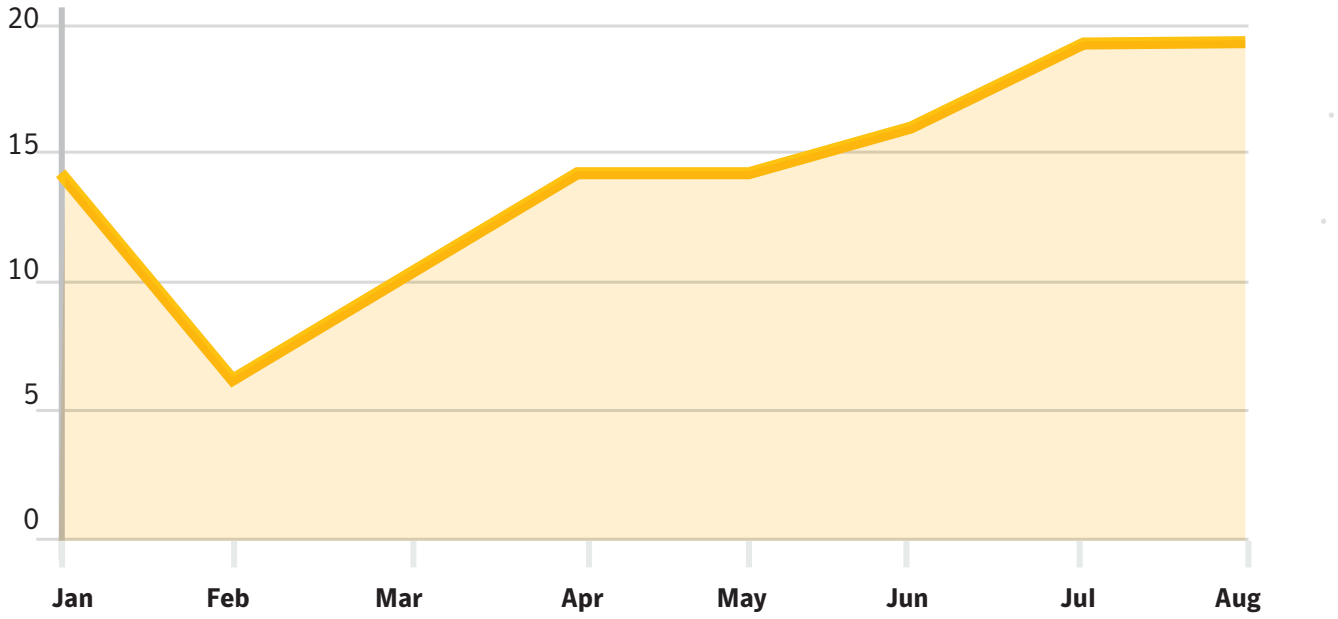


Figure 2: Number of data breaches per month in 2012 to date

Figure 3: Top causes of data breaches by number of identities exposed in 2012 to date

Consequences of a data breach

A data breach in a financial institution can put the business at risk from different perspectives. All of the following issues need to be considered when defining the business case:

- Managing a breach – The process of retrieving data and tracing the breach involves expense and resource.
- Impact on brand reputation – Customers can lose faith in their bank if breaches are broadcast in the media.
- Regulatory fines – Stronger and more impactful enforcement is likely to be seen outside of the US and the UK, where it is already prevalent.

These consequences can be avoided by ensuring that systems are secured and by remaining vigilant so that successful attacks can be remediated before data is breached.

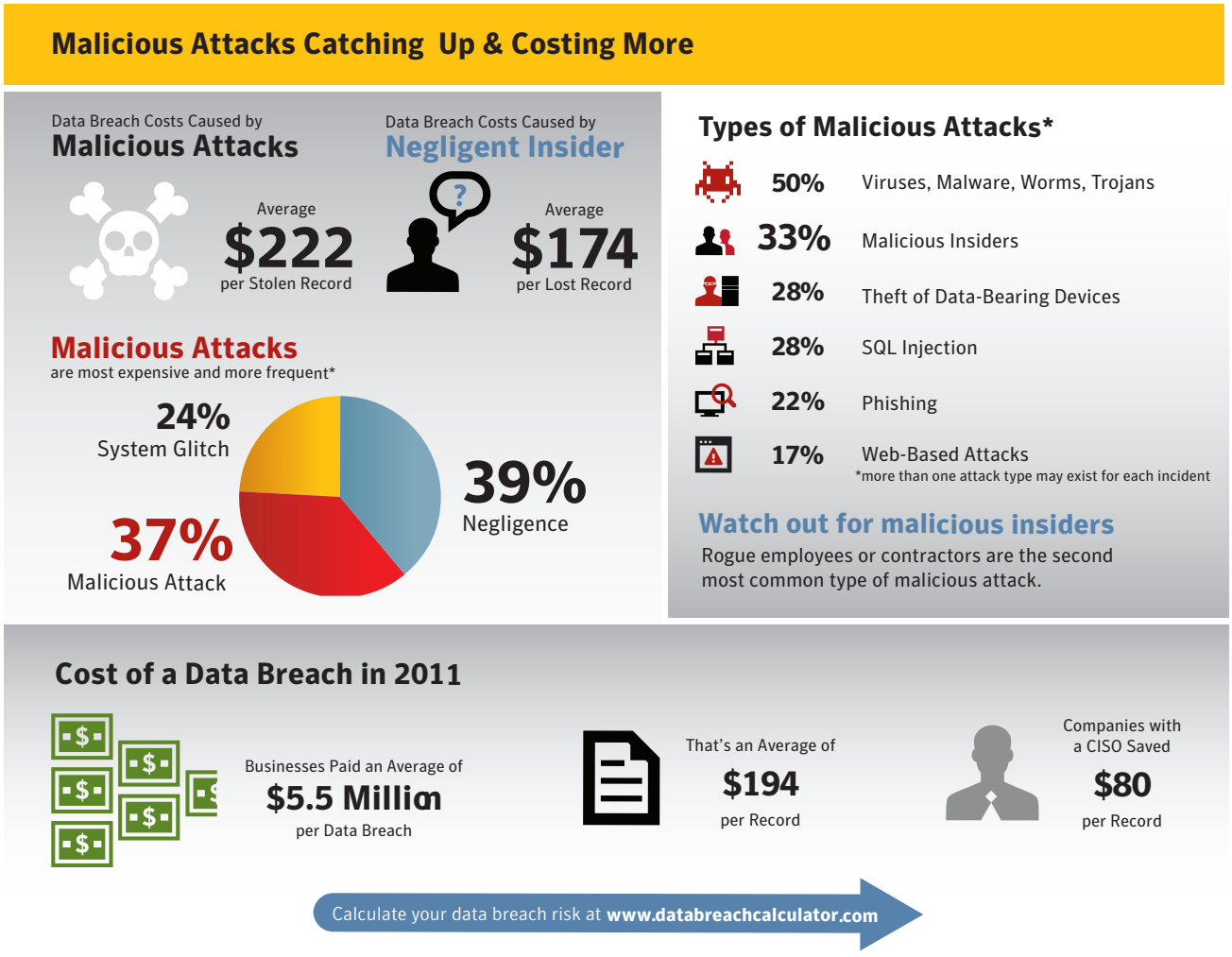


Figure 4: Data courtesy of 2011 Annual Study: U.S. Cost of a Data Breach

Implementing future-proof security

Emerging trends and technology evolution are paving the way for new ways of working, but also for new security threats and challenges. As cybercriminals shift their focus to bank employees and mobile banking gains momentum, the only constant in this game is change. Security strategies and infrastructures need to become more agile and predictive as no technology can rule out the human factor completely, so security awareness will remain critical.

Education of employees is the best defence against many threats. However, this is most effective when organisations break away from traditional security awareness models to employ creative and immersive techniques and deploy technologies that can influence user behaviours.

Automation of processes is a vital part of a future-proof security infrastructure as it helps guard against human error and offers the capability to manage large amounts of data.

Multi-layer security, including firewalls, secure sign-on, dual authentication with triangulation of access and real-time business event monitoring, helps protect against data failings from external attack.

Improved real-time tracking and business intelligence will alert companies to any security breach. The ability to monitor every transaction across global operations will be the key to protecting against internal and external threats.

Managed security services, or a security operations centre, will help detect real-time external or internal security breaches.

New technologies, such as mobile banking applications or payment, need to be considered within the overall security framework. This will be critical from a cost and resource perspective. Applications, procured through line of business functions, can operate outside of the core infrastructure which will impact on the security and risk posture of the organisation.

Recommendations for a secure transition to social, mobile and cloud-based banking

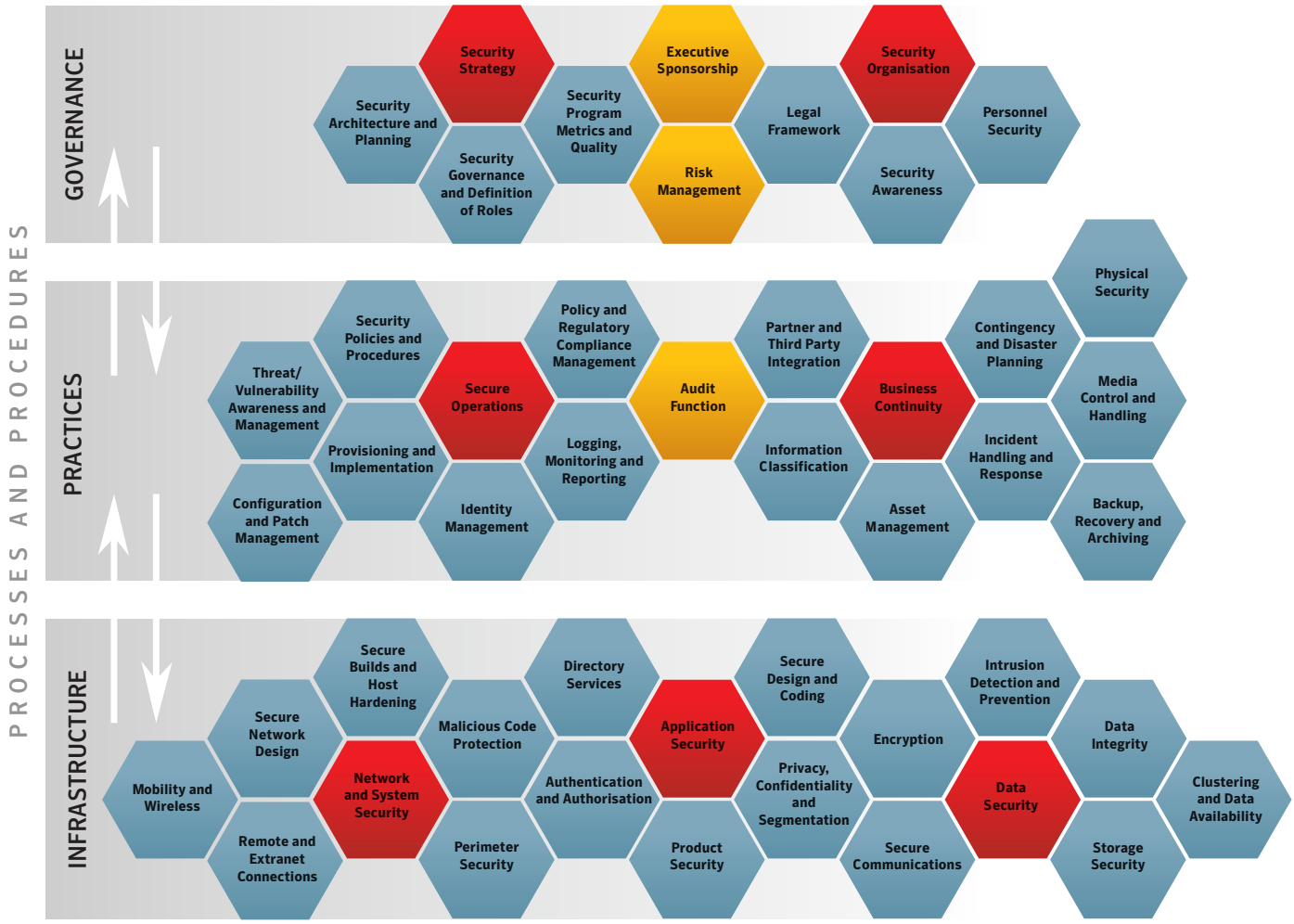


Figure 5: The security framework

The bottom-line is that financial institutions will be unlikely to keep ahead of criminals and so will remain a top target for attacks. To counteract, organisations will need to continuously update information security policies, systems and infrastructures, and ensure they keep up with best practices in securing customers' data.

Governance: Integrating compliance with threat intelligence

The security ecosystem is complex and starts with governance. Banks need to develop and enforce IT policies that comply with regulations, but also ensure that risk is being minimised for targeted attacks against identified critical systems, such as core banking or customer data.

Effective governance requires an integrated approach, which sets the standards on the right level for the different parts of the business. By prioritising risks and defining policies that span across all locations, policies can be enforced through built-in automation and workflow to protect information, identify threats, anticipate and remediate incidents.

Practices: An information-centric approach

The financial services industry needs to take an information-centric approach to identifying and classifying confidential, sensitive data: where it resides, who has access to it and how it is entering or leaving the organisation. Proactively encrypting endpoints will also help organisations minimise the consequences associated with lost devices. To help control access, IT administrators need to validate and protect the identities of users, sites and devices throughout their organisations. Furthermore, they need to provide trusted connections and authenticate transactions where appropriate.

Organisations also need to manage systems by implementing secure operating environments, distributing and enforcing patch levels, automating processes to streamline efficiency, and monitoring and reporting on the status systems. IT administrators need to protect their infrastructure by securing all of their endpoints – including the growing number of mobile devices – along with messaging and web environments. Defending critical internal servers and implementing the backup and recovery of data should also be prioritised. In addition, organisations need visibility and security intelligence to respond more rapidly to threats.

Infrastructure: Bridging legacy systems and high complexity infrastructure

The infrastructure of a bank is a long-term investment and, in many cases, legacy systems also need to be maintained. It is important to ensure there is one security framework which incorporates old systems as well as new resources, such as cloud services, platform services, mobile devices and applications. At the same time, the infrastructure needs to be reorganised to reduce complexity. The latest Symantec State of the Data Center survey demonstrated how infrastructure challenges will have an impact on both security and on data growth congesting systems and networks[13].

Side effects of data center complexity

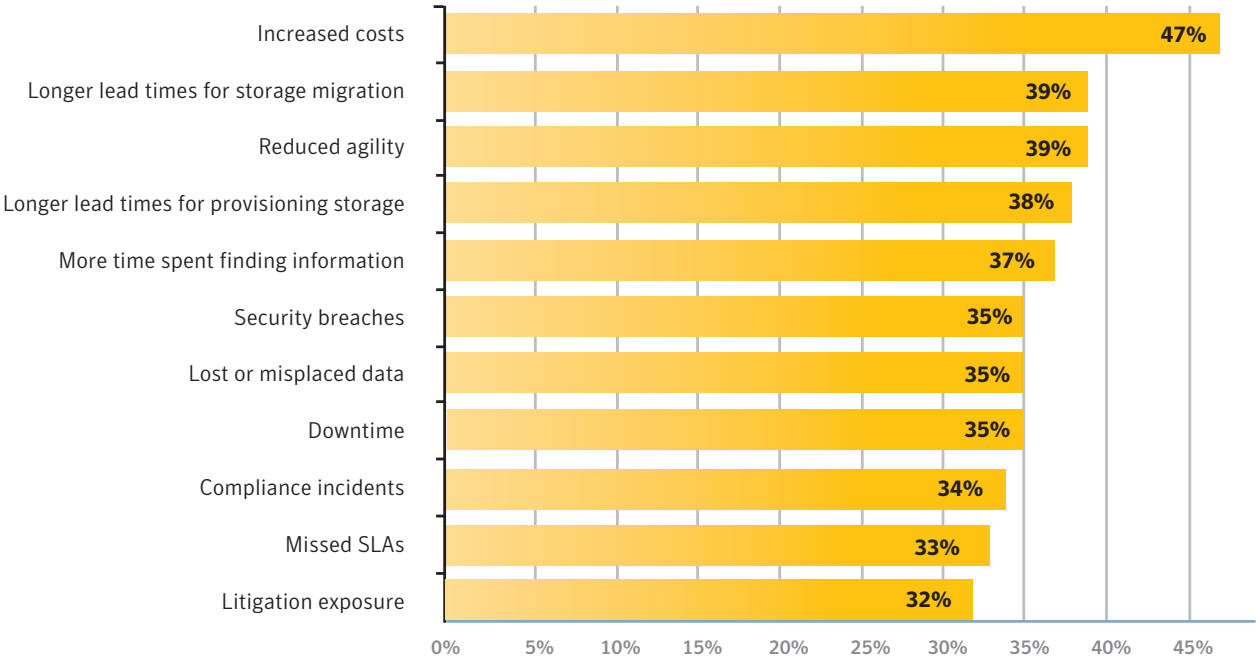


Figure 6: State of the Data Center 2012, Symantec report

Drivers of increasing complexity

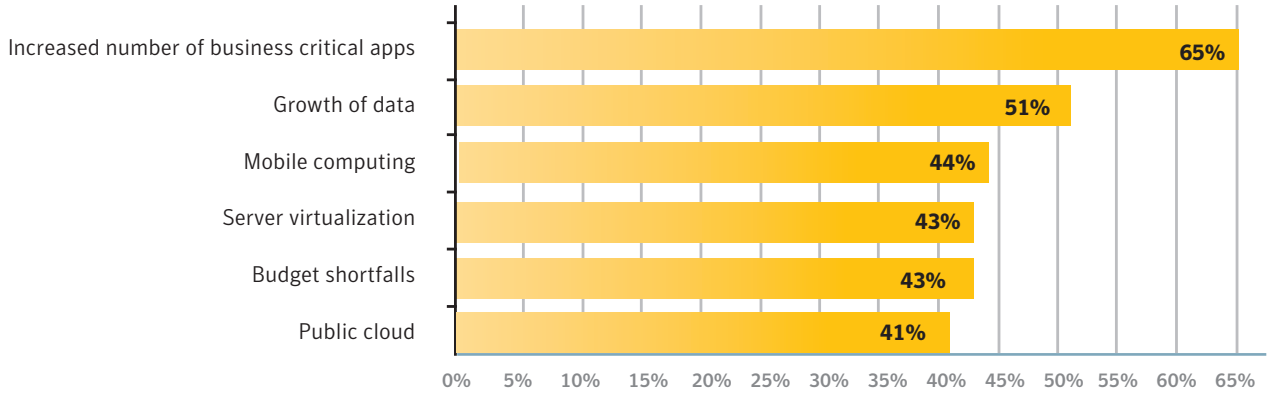


Figure 7: State of the Data Center 2012, Symantec report

Implementing best practices against targeted attacks

There are a number of key issues that financial institutions should consider in order to move beyond a one-size-fits-all approach and begin to successfully fight targeted attacks.

1. Predictive threat analysis

Threat intelligence is a key starting point for any enhanced security strategy. Before selecting an information security tool, institutions should identify their core business processes, classify the information they handle, understand how data flows, comprehend the legal and regulatory landscape they exist within, and then adopt a risk-based approach to setting priorities. By identifying assets, threats and vulnerabilities, this approach allows the qualification and quantification of probable occurrence and impact.

2. Employee training

Due to the extensive list of information security domains, some organisations focus mainly on initiatives around governance: risk and compliance; identity management and access control; data loss prevention; network and information security; and penetration testing. While these five domains set the foundation for information security, organisations should not forget that security processes, tools and infrastructure are defined and supported by people, not machines. Thus, effective awareness programmes and well-trained staff are crucial to cyber security solutions. An internal security task team should work with a trusted security vendor to perform a detailed analysis of risk management. Organisations do not need to hold all the expertise in-house, as specialist skills can be acquired from trusted organisations as required.

3. Identity management

The key to protecting customer information is establishing a stringent identity management programme that implements multi-factor authentication; strong data encryption mechanisms to protect data storage and transmission; and fraud detection and monitoring mechanisms. In addition, when mobile devices are part of the strategy, all associated threats must be identified before granting consumer access to sensitive functions and data.

4. Measurement and reporting

Constructing a well-established metrics programme to effectively analyse the cost-benefit ratio of security solutions is paramount, as it will allow CISOs to articulate the value of security solutions. The cost associated with the security solution can then be compared with the cost associated with the data, assets and overall value in need of protection, thus ensuring the solution does not exceed this value.

5. Test your plan

Test your plan before a breach happens. Security intelligence should enable breaches to be discovered rapidly and stopped at an early stage. Processes and tools, such as backup and data loss prevention, should also be available to recover and restore information.

Conclusion

The finance industry is constantly fighting cybercrime and, given the potential financial gain from a successful attack, this battle is likely to continue. However rigorous the security employed, exposure to new risks is inevitable. New technologies and services must be adopted to cope with competitive pressure and regulations must be complied with. Only by advancing the intelligence and analysis around attackers and their methods, can the industry hope to stay ahead.

The right partner for infrastructure and information protection

Symantec protects information for banks, their employees and their customers. Symantec is a global leader in providing security, storage and systems management solutions to help customers – from consumers and small businesses to the largest global organisations – secure and manage their information and identities independent of device. Symantec brings together leading software and cloud solutions that work seamlessly across multiple platforms, giving customers the freedom to use the devices of their choice and to access, store and transmit information anytime, anywhere.

References

1 Fraud Alert – Cyber Criminals Targeting Financial Institution Employee Credentials to Conduct Wire Transfer Fraud, 17 September 2012

2 U.S. Financial Sector has raised its Cyber Threat Level from Elevated to High, 21 September 2012 http://cyberwarzone.com/us-financial-sector-has-raised-its-cyber-threat-level-elevated-high

3 Citibank Customer Data, Updated Information on Recent Compromise to Citi Account Online For Our Customers, 15 June 2011 http://citigroup.com/citi/press/2011/110610c.htm

4 2011 Symantec State of Security survey, p. 13, August 2011

5 Symantec Internet Security Threat Report 2011 Trends, Volume 17, p. 15, April 2012 http://www.symantec.com/threatreport/

6 Deloitte, 2012 Global Financial Services Industry Security Survey: Breaking Barriers, p. 5

7 Symantec State of Mobility 2012, p. 13, February 2012

8 Symantec Executive Report, Harnessing the Potential of Mobile and Banking, 2012 www.symantec.co.uk/mobileandbanking

9 IDC Financial insights 2012 predictions webcast, 17 December 2011 http://event.on24.com/r.htm?e=388206&s=1&k=16E2F4EABEA09D07B803B0551FF3B1BB

10 Deloitte, 2012 Global Financial Services Industry Security Survey: Breaking Barriers, p. 5

11 M Lee & O Thonnard, Towards A Predictive Analysis of Targeted Attacks, yet to be published

12 Norton Cybercrime Index, (online/real-time index) http://cci-web.finedesigngroup.com/flashApp?stnt=22618:11:0 Report analysing 2011 trends http://us.norton.com/cybercrimereport/promo

13 Symantec State of the Data Center Survey 2012, p. 6, September 2012

Author

Marie Pettersson, Symantec Corporation

Glossary

Targeted Attack

An attack that seeks to breach the security measures of a specific individual or organisation. Usually the initial attack, conducted to gain access to a computer or network, is followed by a further exploit designed to cause harm or, more frequently, steal data.

Advanced Persistent Threat (APT)

Usually refers to a group, with both the capability and intent to persistently and effectively target a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage using a variety of intelligence-gathering techniques to access sensitive information, but applies equally to other threats such as that of traditional espionage or attack. Other recognised attack vectors include infected media, supply chain compromise, and social engineering. Individuals, such as an individual hacker, are not usually referred to as an APT as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target.

Denial-of-Service (DoS)

An attack specifically designed to prevent the normal functioning of a system and thereby to prevent lawful access to the system by authorised users. Hackers can cause denial-of-service attacks by destroying or modifying data or by overloading the system's servers until service to authorised users is delayed or prevented.

ThreatCon

A global security alerting system from Symantec, ThreatCon stands for 'Threat Condition'. ThreatCon is a free interactive tool that alerts users to the current state of global Internet security, providing them with up-to-date information so they can protect themselves against a wide range of online threats.

Symantec Global Intelligence Network

The Symantec security intelligence service that provides global threat information, such as watch lists and threat condition alerts.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec is a global leader in providing security, storage and systems management solutions to help customers secure and manage their information and identities.