Data Breaches: An Inside Perspective

Why Traditional Financial Institutions are Losing the Battle Against Cybercrime
About Omlis

Omlis mobile payment security solutions transform the financial services industry with instantly secure transactions and greatly enhanced customer payment experiences, providing absolute protection that is fraud-free.

Omlis brings to market the first mobile payment solution designed, developed, and tested using high-integrity development processes that are typically used for security-critical applications. Consumer information is no longer vulnerable to attack due to this novel method of encryption.

Learn more at www.omlis.com
Foreword

I am proud to introduce the first report published by Omlis. Our research strategy centers on discovering the problems that exist within traditional financial institutions in order to develop a convenient and all-encompassing method for combating fraud.

To accomplish our goal, we interviewed security professionals with years of experience in combating fraud and data breaches. Through these conversations, Omlis is able to disclose the core issues surrounding information security and provide new insights into why the incidence of security breaches is occurring.

So what did we learn? Increased regulation does not necessarily mean a reduced incidence of security breaches. People will continue to make errors. What is required is a modern security system which minimizes user interaction in order to eliminate the margin of error that leaves so many organizations vulnerable. The complex systems powering the financial services industry need to be simplified, and the risk of breaches needs to be minimized. A new way of thinking is necessary to overhaul outdated practices.

This report examines how financial institutions manage risks and respond to threats and considers best practice for moving towards a greater security strategy in line with the digital age.

I hope our insights are valuable to you and your organization.

Sincerely,

Markus Milsted,
Founder & CEO
Contents

1. Abstract 2

2. Introduction 3

3. Methodology 4

4. Technology 6
   4.1 Infrastructure 8
   4.2 Applications 9
   4.3 Endpoints 10

5. People 11
   5.1 Knowledge, Awareness and Understanding 12
   5.2 Responsibility 13

6. Processes 15
   6.1 Blacklisting vs. Whitelisting 16
   6.2 Data Loss Prevention (DLP) Solutions 17
   6.3 Security Domains 18

7. Compliance 20

   8.1 Pre-Incident Strategies 25
   8.2 Post-Incident Strategies 26
   8.3 External Response 28

9. Summary and Recommendations 29
   9.1 Summary 30
   9.2 Recommendations 31
1. Abstract

This study attempts to understand the security issues that exist within Traditional Financial Institutions (TFIs). Omlis conducted nine in-depth telephone and face-to-face interviews with experienced cybersecurity professionals to understand why cyber breaches within the financial services industry continue to increase year-on-year.

The discussions centered on technology, people and processes; with the goal of better understanding how a typical attack occurs, the difficulties associated with managing risk and the importance of equipping companies with the tools to provide an immediate response.

The findings suggest that many of the security issues that have caused concerns for TFIs in the past are still prevalent today. However, new issues are also entering the fray as a result of advancements in technology and increased regulations.

Taking the above points into account, this paper suggests a new direction for TFIs as a solution to this burgeoning issue.
2. Introduction

The 1950s was the onset of a digital revolution which gave rise to the digital age; a shift from analog, mechanical and electronic technology to digital technology.

The development of microprocessors has been central to this revolution, with steadily increasing performance, computers becoming smaller and more powerful and telecommunications technologies improving speed and wireless capabilities. The result has been mass production and widespread use of digital devices and their associated technologies.

In the late 1980s and early 1990s, laptops first allowed computers to become portable and pagers were largely replaced by mobile phones. In recent times we have seen the introduction of tablets and smartphones.

To meet these changes in consumer use and preference, TFIs have had to invest heavily in upgrading their web and mobile technologies, there are various advantages to do so:

- Firstly, digital technologies increase a bank’s connectivity, not just with customers but also with employees and suppliers.
- Secondly, it allows them to utilize data in a more sophisticated fashion, specifically to conduct advanced analytics and provide increased intelligence for decision making.
- Thirdly, it allows a range of processes; particularly those that are repetitive, low-value, and low-risk to be automated.
- Finally, it is a means to foster innovation across products and business models. The use of technology has made banking faster, with services being provided in real-time.

However, during this time, regulators and methods of best practice have been one step behind. The digital revolution undermined the regulatory framework with which banking was kept under control in the industrial age. This has led to areas of vulnerability within today’s information security systems.

The increase in consumer digital device usage is strongly correlated with an increase in cybercrime. Verizon’s Data Breach Investigation Report (DBIR, 2014) saw a continued increase in the volume of security breaches across industries. The financial services industry saw the highest volume of data breaches in ten years of coverage.

This industry has long been the preferred target of cybercriminals and hackers because of the monetary rewards. It is understood that the rising frequency of attacks is in part due to the increased professionalism of hackers and more sophisticated hacking tools.

We also have an understanding of why a greater number of attacks are being reported, again in part due to the increased number of fraud monitors and greater public awareness.

However, the current issues faced by TFIs are less clear.

This paper attempts to describe the vulnerabilities that exist across the financial services industry, the methods that Information Security departments use and the continuing problems that they face.

For the purposes of this research, the term TFI typically refers to today’s banks that were set up before the boom of the digital age.
3. Methodology

Omlis conducted a series of in depth interviews with security professionals during September and October 2014. Their roles are described below.

<table>
<thead>
<tr>
<th>Consulted Expert</th>
<th>Title &amp; Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adrian Leung</td>
<td>Head of Information Security at Catalyst Housing, former Security Consultant at Deloitte</td>
</tr>
<tr>
<td>Alexis Gargurevich</td>
<td>International Information Security &amp; Privacy Advisor at SixthGale Consulting and former Security Consulting Manager at Deloitte UK</td>
</tr>
<tr>
<td>Bryan Foss</td>
<td>Non-Executive Director, Risk and Audit Chairman at aSource Global and Foss Initiatives</td>
</tr>
<tr>
<td>David Clarke</td>
<td>Chief Technology Officer at Orion Software and Services</td>
</tr>
<tr>
<td>Dr. Darryl MacGregor</td>
<td>Principal Technologist at QA</td>
</tr>
<tr>
<td>Juan Pablo Gonzalez</td>
<td>CEO of Stratus Technologies Mexico</td>
</tr>
<tr>
<td>Paul Johnston</td>
<td>IT Security Consultant / CREST Web App Tester at Pentest, former Security Consultant at a large financial organization</td>
</tr>
<tr>
<td>Richard Sharod</td>
<td>Africa and Middle East Regional Director at Stratus Technologies</td>
</tr>
<tr>
<td>Simon Cairns</td>
<td>Director of Orion Software and Services</td>
</tr>
</tbody>
</table>

Discussions were centered around attitudes and opinions towards cyber breaches, legislation, regulations and compliance, security and prevention measures and incident response management.

Collectively their experience encompasses a range of consultancy roles across Europe, North America, South America and the Asia-Pacific. They have worked for some of the largest financial services organizations and security consultancies in the world.

Interviews were transcribed and analyzed, key themes across interviews were extracted and summarized in this report.
“The biggest danger we talk about is ‘the triangle’ – technology, people and processes. Any one of these can be attacked. Ten years ago it was all aimed at technology, nowadays it can be aimed at either technology or people. Very rarely, but worth mentioning, some will go after the processes.”

Dr. Darryl MacGregor, Principal Technologist at QA
“It’s useful to divide technical security into three pillars: infrastructure, applications and endpoints.”

Paul Johnston, IT Security Consultant at Pentest
4. Technology

Since the introduction and growth in popularity of mobile banking, new organizations that enter the financial services industry adopt a different type of security architecture in comparison to the ones used in TFIs.

Many TFIs have chosen to retain and upgrade their original legacy systems by adding to their existing architecture. This is a trait that distinguishes many modern organizations from their traditional counterparts.

“Look at the encryption systems being offered by Google and Twitter,” advises Dr Darryl MacGregor, a principal technologist at QA. “They are more modern, newer algorithms than those in the financial institutions. Often when we describe this to the security people in financial institutions they think, ‘well, how are we behind the curve?’”

Figure 1 outlines the Three-Tier Architecture security model that is commonly used by TFIs. It is comprised of a data tier, application tier and client tier; which creates an outdated and unnecessarily complex system for managing information security.

Figure 1. The Three-Tier Architecture
4.1 Infrastructure

The data tier is similar to the central nervous system of the human body. It is the most critical part of the overall architecture as it contains highly sensitive and confidential information such as customer records, account information and monetary transaction statements.

These systems were originally designed in the late 1970s and not made for many of today’s modern processes. As their original systems still perform many of their core functions, there is often great apprehension at the thought of changing them.

Many TFIs have been involved in mergers or takeovers and as a result, their respective infrastructures were aligned accordingly. On the surface it may seem a relatively simple process; however, underneath there is an increasingly complex system.

“Banks are very complex organisms and a bank can be a number of acquired companies in one,” David Clarke, Chief Technology Officer at Orion Software and Services explains. “[Difficulties exist] aligning all that infrastructure, as well as upgrading it. So the challenge is, how do we merge all these different companies and then move that into a more advanced platform?”

So would it be advantageous to change their infrastructure? “Nowadays, people tend to do infrastructure security well,” says Paul Johnston, an IT Security Consultant at Pentest. “When you buy a Windows server, it’s well secured out of the box, and the processes to keep it secure are well understood.”

A typical view is, “We’ll keep those systems because we know it works and these lead applications are so critical to our function. That’s a cheaper more robust solution,” explains Dr MacGregor. “Keep it going until it’s financially viable.”
4.2 Applications

The application tier acts as the neurons within the nervous system. It is responsible for transmitting messages or business logic to the endpoint.

As new endpoints are introduced to the existing architecture, TFIs often bolt-on new applications or ‘add-ons’ to allow their customers to use modern electronic devices such as tablets and smartphones.

However, each add-on increases the complexity of an already outdated architectural system. As the complexity increases, so do its vulnerabilities.

Furthermore, each add-on requires business logic or coding to allow the electronic devices to work. For each application there are likely to be errors in the coding that can be identified and pinpointed by skilled hackers.

As Clarke explains, “IT can be kind of flawed. There’s this fact that for every thousand lines of code there’s at least 15 errors. If an architectural system is running potentially hundreds of separate applications then the margin for error is significantly increased.”

“I can’t remember what Windows 8, or Windows 7 had, but I think it had billions of lines of code, so the chances of there being an exploit which hasn’t been discovered is really high.”

Steve McConnell (2004) in Code Complete states, “Industry Average: about 15 to 50 errors per 1000 lines of delivered code.” This is known as the defects per KLOC (1000 Lines of Code).

He goes on to say that “Microsoft Applications have about 10 to 20 defects per 1000 lines of code during in-house testing, and 0.5 defects per KLOC in production.”

Organizations can counter coding errors by using software to continually evaluate their systems. “The companies that do it well, they have training for their developers, they do threat modelling, use tools like DAST* and SAST* and have Penetration Testing*,” says Johnston. “But this isn’t universal.”

*Dynamic Application Security Testing (DAST) is a tool that evaluates how outside sources interact with the application while it is running to find security errors.

*Static Application Security Testing (SAST) is a tool that evaluates information within the security architecture for security vulnerabilities.

*Penetration Testing is an attack on a computer system with the intention of finding security weaknesses.
4.3 Endpoints

The client tier or endpoints are the senses within the nervous system. When we touch an object, information is sent to the brain, when a client logs on to a website; information is sent to the data tier. It is the only area where the client interacts with the organization.

The most common way to breach an organization’s defenses is usually via the endpoints as they represent the weakest element in the security ecosystem.

“Endpoint security almost universally tends to be poor.”

Paul Johnston, IT Security Consultant at Pentest

The reason is often that endpoints operate in an environment outside of the IT team’s control. “It is untrusted networks through the internet that cause the most problems,” suggests Clarke.

Financial institutions cannot continue to utilize their existing architectures long term, as Richard Sharod, Africa and Middle East Regional Director at Stratus Technologies explains, “The longer financial institutions continue to patch* their outdated architectural systems, the greater the risk of misconfiguration, system downtime and breaches.”

---

*A patch is a piece of software designed to update a computer program or to fix or improve it. This includes fixing security vulnerabilities and other bugs, and improving the usability or performance.
“If you go through all the breach reports, from Verizon, IBM, CISCO, Dell, PricewaterhouseCoopers, one of the underlying things is ‘inadvertent human error’, it’s one of the major components of every breach.”

David Clarke, Chief Technology Officer at Orion Software and Services
5. People

Employees handle sensitive data every day and their attitude towards safety is key to ensure a financial institution’s security practices. Failure to meet these stringent security practices could introduce vulnerabilities into their security systems and ultimately result in lengthy investigations, costly fines and significant damage to their reputations.

5.1 Awareness and Understanding

In the past, the difficulty has been ensuring C-Level employees are aware of the security vulnerabilities in their companies.

“If somebody steals your car you know it’s gone; the parking bay is empty. If somebody steals your data, how do you know it’s stolen? It’s still there.”

Bryan Foss, Non-Executive Director, Risk and Audit Chairman at aSource Global and Foss Initiatives

Today, financial institutions are aware of the security implications. The challenge now is ensuring that employees are consistently vigilant and that security remains at the forefront of their minds.

A typical approach is periodic security and awareness training programs, however the impact is most prominent straight after the training and then fades away over time.

“I’ve seen people attend courses and within two weeks they’ve been right in the middle of an incident they could’ve stopped, because the training was ineffective,” says Foss.
5.2 Responsibility

Vulnerabilities can also be introduced by the employees most skilled and experienced at preventing such threats.

Security managers fully understand the importance of installing regular updates to ensure protection against the latest threats. However they are also aware of the associated risks of introducing an error [see System Update Error on page 14].

“They’re schizoid about it,” explains MacGregor. “Some of them detest it. Several TFIs I’m aware of are only now thinking about leaving some their core systems off NT.”

Organizations want a system that automates many of these processes and ultimately takes the risk of a potential catastrophic failure away from them. “Every IT manager wants to go and buy a top of the range anti-virus software and then just carry on as normal, not worrying about malware,” says Johnston.

“The number of APTs* over the past couple of years have proven this approach is not credible,” he continues. And therein lies the problem, “If a network administrator authorized the deployment of a patch and that patch caused business processes to break, they are liable, so people are reluctant to approve anything.” Foss supports this view:

“When deciding whether to deploy the patch, the network administrator thinks: if this breaks something, I’ll get in trouble, if I don’t and there’s some kind of hack I can blame the intrusion prevention system.”

---

*Windows NT is a family of operating systems produced by Microsoft which was first released in July 1993.

*Advanced Persistent Threats (APTs) are computer hacking processes that uses sophisticated techniques involving malware to continuously monitor and extract data over long periods of time.
In 2012 The Royal Bank of Scotland (RBS) Group, which includes National Westminster Bank (NatWest) and The Royal Bank of Scotland, suffered a computer system problem. It occurred through a software update that was applied to RBS’ CA-7 software which controls its payment processing system.

The software upgrade failed, causing a huge backlog of transactions which affected hundreds of thousands of customers.

This caused multiple issues for customers, including:

- Fines for late payments of bills because the system could not process direct debits
- Completions of new home purchases were delayed due to incomplete mortgage payments
- People were stranded abroad without access to money
- A Mexican hospital threatened to turn off a family member’s life support machine because money had not gone through
- One man who was granted bail could not be released from prison as it was unclear if the bail payment had been paid

In November 2014, Business Secretary Vince Cable said the Royal Bank of Scotland’s IT systems were “decades out of date” after the bank was fined £56 million for this computer failure.
Processes
6. Processes

TFIs place extensive resources into ensuring that they can provide the latest innovative products and features to customers. Keeping these products and features secure is often an afterthought, however this should be at the forefront of the development process.

Processes should clearly outline how the technology works, how to use the technology and how information is communicated across departments.

According to Verizon’s DBIR (2014), web app attacks were responsible for over a third (35%) of breaches for data disclosure in 2013 within all industries and over a quarter (27%) of attacks within financial institutions.

In this section we discuss some of the policies that financial institutions employ to reduce the incidence of web attacks.

6.1 Blacklisting vs. Whitelisting

Blacklisting is the process of restricting access to email addresses, websites, applications or software that is deemed untrustworthy. It is a common protection method against attacks in financial institutions; however, there are known vulnerabilities with this approach.

Dr MacGregor explains a relatively simple method that hackers use to sidestep blacklisting, “I would build what I was going to do then I would register a domain name now and send you the email. How is that going to be blacklisted? The site didn’t exist until two minutes ago.”

An alternative approach is whitelisting. “The default status is you can’t see anything.” He continues, “It asks questions such as, ‘why are you going to look here?’ If you can’t provide a business reason, you’re not going to access the website.”

In principle, this method can stop all attacks, but in practice it is a difficult process to manage. “Whitelisting is less popular, as it alienates legitimate users who are used to relatively untrammeled internet access,” says MacGregor.

Furthermore, compiling and maintaining the initial whitelist requires the IT department to review each website, application or piece of software that each department, manager or employee wants to use, to ensure that it meets the organization’s security requirements. It is a prolonged process that can stifle innovation, early adoption of new technologies and may create feelings of distrust amongst employees.
The issue of Bring Your Own Device (BYOD) is an increasingly important one. Allowing employees to use their own devices in and outside of the workplace provides many advantages to organizations such as improved productivity, ‘anytime’ and ‘anywhere’ access and increased employee satisfaction.

However, access to data on devices outside of an IT team’s security boundaries can open the possibility for attacks. The topic of BYOD is a divisive one. “Half the security team is saying ‘we can’t allow it’ and half says ‘we’ve got to’,” says Foss. So there is a dichotomy in many organizations.

According to a 2012 Good Technology survey, 76% of companies with 2000 or more employees were already formally supporting BYOD programs. Another 13% said they were planning to support such programs within a year. Figure 2 highlights the prevalence of BYOD within the financial services industry.

A solution to prevent unintentional data leaks outside of the workplace is to implement an automated corporate policy that will catch protected data before it leaves your organization. This is known as a DLP solution.

“For DLP, you try to understand the different classifications of document. It will allow someone to put some artwork for printing on to a USB stick, but it will forbid them from putting a spreadsheet of customer data on the USB,” says Johnston.

This option is based on a data-classification scheme that specifies appropriate use of that data. Data that falls into the highest categories could be highly sensitive and, if disclosed, could put the organization at financial or legal risk. Data classified in the lower categories could be information which can be freely disclosed in the public domain. “That seems to work well where it’s deployed, but it’s not universal,” says Johnston.

“The usual policy is that people are allowed a virtual desktop on their own device but they’re never allowed to have corporate data on their own device,” explains Johnston. The problem is that employees typically demand flexibility with how they work.

Verizon reported that in 2013, 7% of attacks were related to insider misuse. Employees can apply a variety of techniques to overcome restrictions if they wish such as taking screenshots of data or encrypting files. It is all dependent on how robust the process is.

Another potential vulnerability in DLP solutions is that end users need to ensure that all of their devices are updated in real time. This ensures that their device contains the latest security patches, in order to protect them from the latest threats or exploits. However, “You can’t mandate that everyone’s on a certain release, running a certain version of software, which adds another level of complexity,” says Clarke.
6.3 Security Domains

Computer networks allow terminals to pass information to each other along networked links. They typically allow users to share access of information via storage servers, printers and fax machines or instant messaging apps.

Domain network policies isolate domain member computers from non-domain member computers. To access a specific domain, the domain member computers only accept incoming communication requests from computers that can authenticate themselves with domain credentials.

Financial services organizations typically use logical domains i.e. two domains which run on the same network. Therefore, there is always a possibility that a breach into one network could be used to gain access to data on another [see Escalation of Privilege on page 19].

A physical domain approach is used in military and intelligence organizations, providing employees with two separate computers and running on two separate networks. Johnston believes this could be deployed in the financial services sector. “Certain organizations publicly claim they do this and essentially what you have to do is split your entire IT into two halves; you have a low-criticality network and a high criticality network.”

“They’ve got one general purpose computer to access the internet so they can email their colleagues about non-sensitive issues, and when they switch to their other computer they are in a highly secured inner-enclave, and in that environment they cannot access the internet,” explains Johnston.

Because the two domains run on entirely different networks and are physically separated, it is not possible to gain access to one through another. “That kind of deployment can credibly stop malware, but I’ve not seen it implemented large scale,” says Johnston.
Below we run through the stages of a typical escalation of privilege attack, as explained by Dr. Darryl MacGregor.

1. To start a breach through social engineering, the hacker sends an email containing known malware to the financial institution. An automatic response is received, which may say ‘This was rejected by…’ informing the hacker which malware detection software the target organization is running.

2. Next, the hacker would produce a piece of malware, possibly using some kind of kit, encrypt it, expose it to that machine and see if the defenses are triggered. If they are, the hacker will keep re-encrypting the malware and exposing it to the anti-malware software until it doesn’t trigger, meaning it would also not trigger the target machine’s detection systems.

3. An apparently innocuous email is then sent to the organization with an attachment, typically a .pdf file, containing the encrypted malware. The malware intrusion detection systems are signature reliant in most cases and because the malware is encrypted, it does not set off the intrusion detection system. Buried inside the .pdf file is something that will take over the target machine, exploit a vulnerability and give the hackers control of that device. The .pdf file is used a lot because it is such a good container. If hackers can get the target to click on this, they then have control of a machine which is inside the target environment.

4. Hackers will then often employ a keystroke logger which records the keys that are pressed on the machine and can cause a trivial but annoying fault (e.g. a script that changes the screen resolution). By setting malware on a computer that the target can’t change back, it is likely that they will then contact their IT department for support.

5. With a keystroke logger working on the target’s machine (e.g. winlogon.exe) it will record anything that is typed into the machine, directly or remotely, allowing the hacker to obtain names and passwords of employees with administrative privileges. Hackers can then go into another system, insert those credentials and see what access they provide. If necessary, hackers can repeat the scam at a higher level until eventually they have a domain administrator’s details.
“Being compliant doesn’t guarantee that you will be secure. The importance given to checklists and tick boxes at times reduces our ability to apply common sense.”

Juan Pablo Gonzalez, CEO of Stratus Technologies Mexico
7. Compliance

Financial institutions are supported in their attempts to keep data secure through standard organizations, who outline methods of best practice and governing bodies, who influence regulations within the industry.

“The government have produced some security guidelines called Cyber Essentials and the SysAdmin, Audit, Networking, and Security (SANS) Institute gives recommendations based on a similar concept of what should be a baseline in terms of boundary security, malware security, patching and access control,” says Clarke.

Compliance can bring major benefits to organizations such as keeping data secure and thereby improving their reputation amongst stakeholders. “The Payment Card Industry (PCI) is a good example. It mandates specific technical and procedural controls. This avoids protracted debates within organizations as the standard makes clear what action is required,” says Johnston.

Conversely, non-compliance can lead to data being compromised; damaging reputations and ultimately resulting in law suits, insurance claims and fines. Because of this, financial institutions place a great deal of importance on meeting standards whether they are mandatory or voluntary.

As Alexis Gargurevich, International Information Security & Privacy Advisor at SixthGale Consulting explains, “Financial services are ahead of the curve. You’ll find that most will have some certification already, whether it’s ISO: 27001* or PCI DSS*.”

The result is that, “We are working in a highly regulated environment, not only because of the regulations but also best practices and industry standards, which every company would like to be aligned with,” continues Gargurevich.

The way that you secure data for one set of standards can often be useful in meeting the standards of another. However, there are issues born from the sheer amount of standards that organizations can choose from. “Some regulations are vague,” says Johnston. “Sometimes the regulators tell them to do things which are actually distracting in terms of time, money, effort and results,” adds Foss.

Other issues include over-reliance on standards.

“A lot of people become compliant and think that’s how to improve. They read something like the PCI DSS compliance and they’re finished. That’s it for the year.”

Dr. Darryl MacGregor, Principal Technologist at QA

---

*International Organization for Standard (ISO) 27001 is a specification for the legal, physical and technical controls involved in an organizations information risk management processes.

*Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.
“I think that too many people look at the regulators for the answers instead of looking inside their own business,” explains Foss. “The more the regulator polices the situation instead of passing the responsibility back to the company, the more this is encouraged.”

Foss is aware of poor security practices despite achieving compliance. “I’ve been into situations where a couple of months before a major event happened, they’d just completed an ISO: 27001 audit, receiving a completely clean sheet.”

“Looking around I found time bombs all over the place ready to go off,” he continues. “Why weren’t these picked up? They were trying to look as though they’ve done something but they weren’t really serious about it.”

However, a succession of high profile cases may be changing the attitudes towards compliance. “It’s made people worried, just because you’ve got the standard it doesn’t necessarily make you secure,” says Clarke. “They [Target] were certified as PCI DSS but they were compromised by a kind of malware and on top of that, it compromised another 1000 suppliers.”

Case Study: Target Breach

Target, the third largest retailer in the US was the source of the biggest retail hack in the country’s history. Between 15 November and 28 November 2013, malware was installed in Target’s point of sale (POS) devices across the company’s 1,797 stores. When the customer’s card was swiped for payment, the malware would capture the credit card number and store it on a Target server commandeered by the hackers. Between 27 November and 15 December 2013, 40 million credit card numbers and 70 million addresses and phone numbers had been breached.

Target Chairman, President, and Chief Executive Officer Gregg Steinhafel issued an email statement: “Target was certified as meeting the standard for the payment card industry in September 2013. Nonetheless, we suffered a data breach. As a result, we are conducting an end-to-end review of our people, processes and technology to understand our opportunities to improve data security and are committed to learning from this experience.”
“Depending on how prepared a company is to deal with a threat and also the risk, they may have to ask themselves: ‘Do we get the police? Do we talk to our customers? Do we turn our website off?’”

Paul Johnston, IT Security Consultant at Pentest
8. Information Security Management Systems (ISMS)

ISMS are a set of policies concerned with information security. The principle is that organizations should design, implement and maintain a set of policies, processes and systems to manage threats.

To exercise effective ISMS, employees throughout the organization must clearly understand their information security strategies and how to act to both prevent and respond to an attack. This requires effective communication.

“In small businesses, you normally find that there are several people who understand the entire operation and if they’re going to make a particular decision they understand all of the competing, conflicting requirements of different parts of the business,” explains Foss. “They know that they need to get it done and they need to be secure, so small businesses tend to make intelligent decisions.”

However, the same is not necessarily true for large companies. “You have a security team and you have a networks team, a workstations team and a web team who all have their own requirements,” he continues. “They often don’t think about the other team’s requirements, so there is an overall view that people just work in isolated silos.”

“Companies tend to place extensive resources into the more complicated aspects of security to minimize risk. However, data breaches are often the result of straightforward issues that could easily be controlled, yet are repeatedly taken too lightly,” explains Simon Cairns, Director of Orion Software and Services.

“Monitoring also needs to be done by people who are not doing the operational job themselves. Those are the people that could commit fraud because they can do stuff which you don’t understand,” Foss explains. “A few privileged staff are right in the center of your systems and they are running the monitoring as well as running the changes. So one of the things you have to do is separate the changes from the monitoring, you cannot have those two things combined to be secure.”

“What if you’re outsourcing it to another country? To another business?” He continues. “You don’t know whether they’re using contractors, whether they’re trained, who they are.”

In this section we describe the pre and post-incident strategies that are typically employed by TFIs.
8.1 Pre-Incident Strategy

The frequency and intensity of cyber-attacks makes it very difficult for TFIs to combat all threats. Managing risk is not an exact science, therefore TFIs typically opt for a strategy that focuses on the most likely and most impactful types of attacks.

“You need to look at the things about your business model which are unique and decide where the risks lie. Then you need to look for the regulations and other things that will help you to improve,” says Foss.

Figure 3 outlines the Probabilistic Risk Assessment (PRA) approach used by financial institutions to identify the greatest risks to their organization. It is based on organizations asking themselves three types of questions:

1. What can go wrong?
2. How severe would the implications be?
3. How likely is it to occur?

Risks are calculated using the following formula:

\[
\text{Likelihood of an incident occurring} \times \text{Impact of that incident on the organization} = \text{Overall Risk}
\]

Risks that fall within the red category are considered high risk, those within the amber category are medium risk and those within the green category are considered low risk.

“If the score is bigger than say 15, the board need to review it on a monthly basis,” says Foss. “However they also need to continually monitor the risk factors given at amber as these threats constantly change, so the perceived likelihood and / or impact can also change.”

The PRA approach cannot account for unknown threats or what the more cunning hackers are able to do. “The professionals take three semi-vulnerabilities and connect them together. That’s the big difference, the less experienced will go for the obvious route, they’ll go down route one. The professionals will be able to put several routes together to gain access to the resource,” Dr. MacGregor explains.

An example is given below:

An inexperienced hacker may target:

1 x factor with a high likelihood (4) but with very low impact (1) = overall low risk factor of 4

A professional hack may target:

4 x factors with a high likelihood (4) but with very low impact (1) = overall low risk factor of 16

High risk factors are often not the main point of attack, as Adrian Leung, former Security Consultant at Deloitte explains. “Why would an adversary try to attack or breach a HSM* if there are other easier routes of entry?”

<table>
<thead>
<tr>
<th>Impact</th>
<th>Very Low (1)</th>
<th>Low (2)</th>
<th>Medium (3)</th>
<th>High (4)</th>
<th>Very High (5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Low (1)</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Low (2)</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>Medium (3)</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>15</td>
</tr>
<tr>
<td>High (4)</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>20</td>
</tr>
<tr>
<td>Very High (5)</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>25</td>
</tr>
</tbody>
</table>

**Figure 3. The Probabilistic Risk Assessment Model**

*Hardware Security Modules (HSMs) are dedicated crypto processors that are specifically designed for the protection of the crypto key lifecycle and to secure the most sensitive of data. The potential impact of a HSM breach would be very high.*
8.2 Post-Incident Strategy

An incident response plan is an approach to addressing and managing the aftermath of a security breach or attack. The aim is to handle the situation in a way that limits damage and reduces recovery time and costs.

“When data protection is mandatory you need to report it to the Information Commissioners Office in the UK,” says Gargurevich. “If you’re a bank and you’re issuing credit cards, then you’re aligned to the PCI and therefore you need to report the breach to the PCI Council, as well as the merchants and your card provider whoever it is.”

“If you don’t do that, and let’s say Visa or MasterCard find out that you failed your PCI certification, then you get a fine, it could be at least £250,000 to £300,000,” he continues. “So you need to know how many customers have been affected and you have to be able to roughly know for how much time this has happened.”

Figure 4 highlights the Incident Response Life Cycle by The National Institute of Science and Technology (NIST).

During preparation, the organization attempts to limit the number of incidents that will occur by selecting and implementing controls based on the results of risk assessments [see Pre-Incident Strategy on page 25]. However, residual risk will inevitably persist after controls are implemented.

Early detection of security breaches is necessary to alert the organization whenever an incident occurs. The organization can mitigate the impact of an incident by containing it and ultimately recovering from it.

After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents.
Below, Gargurevich describes a step-by-step incident response plan:

1. Try to keep those locked files as secure as you can because those are your sources about how the attack actually happened.

2. Next, replay the attack or you won’t be able to actually stop the attacker. Investigate their system just like a hacker would and see if there is a way to cause a similar breach.

3. Block it immediately. The only way to block it is to know exactly which files are affected and stop that happening without disrupting the services. You don’t want to just shut down everything, you need to know exactly where it is.

4. In the time this has happened we would recommend a technical change to the website, which means that the website can be kept on but they can also be confident they won’t have a further breach.

5. Investigate the vulnerability:
   a. If there was a web server with a vulnerability, you need to know what your vulnerability is and stop it. You could use a firewall to stop that network traffic or essentially get in a server patch in that moment and stop that traffic coming.
   b. If it’s a virus then try to isolate that part of the network.
   c. If it’s a data loss incident then tighten things up and prevent it from going everywhere. For example, if an employee is losing things, then DLP is critical and they must tighten up their processes to ensure that nobody else compromises company data.
   d. If there is a disruption of services, for example, a Denial of Service (DOS) attack, where your website will be brought down by the number of requests, most companies will definitely restart their service but also try to define from where the traffic is coming in.

“Without a plan in place you’ll need to wait,” explains Gargurevich. “If you have a clear plan of what to do, you should have the right contacts to get hold of the Internet Service Provider who hosts that server and request that server to be brought down.”

Ultimately, the success of an incident response plan is dependent on the strength of processes that are in place. What if a company has no contingencies in place? “Up to a certain amount they might as well just take the loss and the problem goes away. On many occasions you’ll never catch them. They may not even be in European or US jurisdiction, they could be in Asia or Eastern Bloc,” explains Clarke.
**8.3 External Response**

“**You should have a plan to act internally on who needs to do what, who needs to talk to who,**” explains Alexis Gargurevich.

In the US, 47 states have enacted legislation requiring private or government entities to notify individuals of security breaches which involve personally identifiable information. A similar law does not currently exist within the EU and therefore there is no legal obligation for data controllers to report breaches of security which result in loss, release or corruptions of data.

“The bank could work with the police while brushing it under the carpet. Many UK banks offer an online fraud guarantee and by maintaining that guarantee, fully discharge their legal obligations to their clients,” says Johnston.

Aside from the negative impact on reputation, part of the reason why organizations want to keep breaches under wraps is that they have to perform their due diligence under the watchful gaze of the public.

“When your customers become aware, then you potentially need to be prepared to do a Data Subject Access Request*. That is a very painful process for an organization to do because potentially you will need to furnish them with all the information that you have about them in structured and unstructured correspondence,” says Leung.

Financial institutions typically avoid this and the subsequent damage to their brand by playing down serious breaches as minor incidences.

---

**Case Study: eBay Breach**

David Clarke describes a recent incident where eBay’s failure to act decisively escalated a breach. “**They breached a lot of passwords. eBay never released this information until three months after the breach. Therefore customers didn’t have an opportunity to change their passwords, giving the hackers an opportunity to scale up their attacks.**”

“At the time I was thinking, that’s interesting, I think a lot of people’s eBay accounts are linked to their PayPal account. How likely is that if you have someone’s eBay password, you also have their PayPal password?” He continues, “**Passwords can be profiled now... All it takes is for one password to be compromised. If their password was for example: ‘password’, the chances are their second password would be ‘password1’ or ‘01’ or ‘02’.**

“You only need two or three of those exposed passwords and you can individually profile people’s password methodologies,” explains Clarke. “**Take that a bit further, the chances are those people work for a company and that company might have interesting data that they [the hackers] want, and there’s a chance those people are using the same passwords at work. The possible knock on effects are huge.**”

---

*A Data Subject Access Request (DSAR) is a written, signed request from an individual to see information held on them. The Data Controller has 40 days of receipt of the request to provide all such information in a readable form.*
Summary and Recommendations
9. Summary and Recommendations

9.1 Summary

Technological innovations and changes in consumer habits since the late 1970s have had a huge influence on the products, processes and services that are provided by financial institutions.

Today, many TFIs use the same legacy systems that they were using 40 years ago. Each time a new product, process or service is required, TFIs face a choice. They can either add a bolt-on to their existing architecture or overhaul their systems with a modern fit-for-purpose system.

Strategic decisions are often driven by an organization’s ability to meet the demands of their customers. Companies will seek a quick go-to-market strategy to aid their reputation as market leaders and also provide an advantage over their competitors.

Adding a bolt-on application to an existing system is often the quickest route to market in the short term. In addition, it allays concerns that financial institutions have about causing interruptions to core business processes and introducing errors.

However, repeatedly selecting the bolt-on approach creates an increasingly complex system which gradually requires greater manual input for maintenance and updates. As the level of manual interactions increase, so do the possibilities of human error and fraud.

Further exacerbating the issue; processes such as whitelisting and physical security domains are often deemed impractical to input; training has a shelf life and in-depth pre and post-incident strategies are entirely dependent on the commitment of employees and the consistent flow of communication throughout an organization. So what is the answer?
9.2 Recommendations

TFIs should seek:

- To employ a software solution that can be deployed immediately and that causes minimum system downtime or disruptions to business processes.
- A solution that is highly interoperable with a range of current applications and backwards compatible with existing applications.
- To incorporate a system that offers immense scalability in order to accommodate the predicted growth in mobile use as many of today’s processes move towards a mobile platform.
- A move towards a system that provides a secure cloud hosting solution. This would solve many of the maintenance limitations that financial institutions with traditional in house server infrastructures encounter. Additionally, a cloud hosting option will provide immediate system updates, thereby reducing human error, time delays and fear of making errors; while offering guaranteed compliance as updates are provided immediately.

Finally, TFIs should seek an endpoint focused solution to improve the security of the weakest and most vulnerable areas of their security systems.

This can be done by offering one-time encryption keys that secure data transmissions from the endpoint across the entire architecture, providing unique and time sensitive authentication tokens and placing authentication in the endpoints. The benefits of which are:

1. The endpoints become as safe as the most critical security applications, such as air traffic control, military, aviation and nuclear safety; and thereby significantly reduces the likelihood of a breach.

2. If a hacker does successfully breach an endpoint, only the data housed in that particular endpoint is compromised, rather than the countless amount of data that is stored by TFIs at a single point within the traditional in-house server infrastructures.

Without such measures, TFIs will continue their unsuccessful attempts to balance innovation and security, using technology that was designed to do neither.
Omlis strives for a future where anyone, anywhere, can use their electronic device and safely conduct any commercial activity with complete and absolute confidence that their activities are fully secure and uncompromised.

Omlis is working with financial institutions and technology distributors to provide complete security and immense efficiency across organizational processes.

We offer a powerful and innovative secure payments technology specifically designed to address the major issues that impact on today’s mobile payments market, most importantly, the massive cost of fraud.

To learn how Omlis technology resolves the issues revealed in this report, watch our webinar, “Securing Legacy for the Mobile Channel” at www.omlis.com/omlis-media-room/webinar-securing-legacy-systems-mobile-channel/

For more information:
Call: +44 (0) 845 838 1308
Web: www.omlis.com or www.linkedin.com/company/omlis
Email: info@omlis.com

Contributors

The following individuals contributed to this report:

Alton Morgan
Researcher - Project Leader

Emma Thompson
Partner Marketing Executive

John Patterson
Copywriter

Jessica Wilkinson
Communications Intern