The Olswang Cyber Alert

June 2014

OLSWANG

Introduction and welcome

Welcome to the first edition of Olswang's Cyber Alert, a regular round up of regulation, best practice and news from our international cyber breach and crisis management team. In each edition:

- we will feature a longer article with commentary on a topical cybersecurity issue. In this edition, we consider cyber breaches in the retail world and the impact of the Target data breach
- we will include updates on the latest security standards and benchmarks
- we will report on the progress of the controversial draft General Data Protection Regulation and the Network and Information Security Directive
- we will keep a watching brief on other cyber liability issues.

In the last few months we have seen news headlines ranging from state-sponsored hacking, arrests over the BlackShades malware, and the release of the latest Information Security Breaches Survey, not to mention continued concern over the Heartbleed vulnerability, so there is much for businesses to consider. See here for a summary of some of the latest headlines.

It is also worth mentioning the European Court of Justice's ***Google Spain*** ruling in May, which is arguably the most profound internet case of this decade and which continues to send shockwaves through the tech sector. Whilst *Google Spain* does not relate to cybersecurity specifically, it does establish that in some circumstances a non-European company is answerable to the European courts and accountable under European data protection laws, including the requirement for appropriate technical and organisational measures to be in place to protect personal data. Read Olswang's update on *Google Spain* here.

We hope you'll find our update useful and we welcome your feedback – but if you'd prefer not to receive future mailings, please use the opt-out link on the covering email.

Ross McKean
Head of Data Protection
Olswang LLP

Cybersecurity and corporate crisis in the retail industry: analysis of the Target security breach

In December 2013 it was revealed that Target, a major retailer in the US, was affected by a security breach. We explain what happened, the likely impact and why proactive security management should be a top priority for retailers.

What happened and how has Target reacted?

No official explanation has been provided, but reports suggest that hackers gained access to Target's point-of-sale (POS) systems following an email phishing attack aimed at one of Target's third party contractors. The hackers then stole the credit and debit card data of up to 40 million customers when sales were made, and personal information relating to up to 70 million customers was also compromised. These numbers were particularly high as the security breach occurred over a three week period in the run up to Christmas.

On discovery of the breach, Target appointed experts to carry out a forensic investigation of its systems. It is also co-operating with U.S. Secret Service and Department of Justice investigations and has:

- communicated with its customers in various ways about the breach, including by email and by having a dedicated area of the Target website with updates, advice and FAQs;
- offered its customers 10% off all sales the weekend before Christmas, plus one year of free credit monitoring and identity theft protection;
- informed its customers that they have no liability for the cost of any fraudulent charges arising from the breach;
- initiated the creation of and invested $5 million in a campaign with a number of other organisations to educate the public on cybersecurity and consumer scams; and
- participated in the launch of the Cybersecurity and Data Privacy Initiative, a retail industry initiative to improve consumer privacy, cybersecurity and payment security.

How was Target's business affected?

The impact of the breach on Target serves as another reminder of how a cyber-attack can turn into a full-blown corporate crisis:

- in March, profits were reported to have fallen 46% (for the same quarter compared to the previous year) and a profit warning has been issued for 2014;
- in February, Target said that its costs to date – including the costs of investigating and managing the breach, paying for credit monitoring services for its customers, additional customer services personnel and legal fees - were $61 million;
- class action lawsuits have already been filed, and more lawsuits and enforcement action may be on the horizon;
- Target's chief information officer resigned in March;
- in March Standard & Poor's downgraded Target's credit rating, partly due to the data breach and its financial consequences;
- Target's CEO resigned in May.

What should other retailers think about in light of the breach?

Like many retailers, Target had taken steps to protect the security of its systems, payment card data and customer information. Despite Target having invested heavily in security, with multiple layers of security protection in place and its certification as compliant with the Payment Card Industry Data Security Standards as recently as September 2013, the cyber-attack still happened.

As Michael Kingston, CIO of another US retailer Neiman Marcus which experienced a similar hack last year, said in February: "*just having the tools and technology isn't enough in this day and age…These attackers again are very, very sophisticated and they've figured out ways around that.*"

However, organisations should still be carefully managing and stress testing their systems on a regular basis to ensure the best levels of security.

Ross McKean, Head of Data Protection at Olswang, commented: "*it is extremely difficult in our hyper-connected age for an organisation to completely safeguard against a security breach; determined hackers will ultimately find a way around security protocols and the most common breaches are often the simplest, such as phishing emails. But because of the huge reputational damage a breach can cause, it is vital for organisations to do - and be seen to be doing - everything they can to protect the security of their systems and data*."

A catalyst for improvement?

The Target breach will impact the US retail and banking industries beyond an individual organisation level.

One outcome will be greater collaboration across the retail industry, with several large US retailers (including Target) now taking part in an initiative called the Retail Cyber Intelligence Sharing Center which allows them to share intelligence about cybersecurity with each other and with security analysts and agencies.

The breach may prove to be a catalyst for greater spending on security across the retail sector. The recent PWC Information Security Breaches Survey indicated that on average UK retailers only spent 6% of their IT budget on security, and various studies suggest that the percentage for US retailers is even smaller.

In the US, the Target data breach is also expected to encourage speedier adoption of more secure technologies for payment cards and systems, where the most common payment system relies on magnetic strips and signature verification for security.

In March, MasterCard and Visa announced a new cross-industry group to focus on enhancing payment systems security, with Visa's president Ryan McInerney specifically referring to "*recent high-profile breaches [serving] as a catalyst for much needed collaboration between the retail and financial services industry on the issue of payment security*". One of the tasks for the group will be the advancement of EMV chip technology (which is widely used in Europe) in the US. This technology generates a unique code for every transaction and therefore has the potential to significantly reduce financial loss due to lost or stolen cards. In the UK, high street losses reduced by 67% in the three years following the introduction of chip and pin technology in 2004.

To effect this kind of change, US retailers need to update their systems and purchase the appropriate hardware to read payment cards with chips. There is a separate incentive for them to do so, as from October 2015 US retailers who haven't upgraded to EMV chip technology will be liable for any fraudulent transactions made using a swipe card issued by the major payment networks (including Visa and MasterCard).

Target has announced that it has accelerated work on a $100 million project to build chip technology into its own payment cards and in-store payment systems. However, other retailers still need to be convinced that the savings will outweigh the investment costs. US banks would also have to start providing more chip cards – it is estimated that less than 2% of the US population own a chip payment card.

Standards and benchmarks

Cybersecurity standards and benchmarks

New ISO standards for cloud service providers

There is a seemingly unstoppable shift of data from old “on-premise” solutions to the cloud. There have been many calls to find an information security standard for cloud service providers. The International Organisation for Standardisation ("**ISO**") has announced the development of two **cloud specific standards, ISO 27017 and ISO 27018**. The two standards are due for official release in 2015. You can read more on these standards in the Olswang Datonomy Blog here.

New cloud security guidance

The Communications-Electronics Security Group ("**CESG**"), the information security arm of the GCHQ, has also recently published a Risk Management Guide as part of its Cloud Security Guidance. The Cloud Security Guidance is aimed at public sector organisations, but is equally useful for private enterprise. The guidance takes the form of a seven step approach for risk management when assessing and using cloud services. The seven steps are (1) know your business requirements; (2) understand your information or application; (3) understand which security principles your service implements; (5) understand what assurance is available in their implementation; (6) consider what additional mitigations consumers can apply; and (7) consider whether the remaining risks are acceptable.

Top security threats and how to avoid them – a new report from the UK ICO

In May, the ICO published a report which identified eight common IT security threats which have commonly arisen during the ICO’s investigations into data breaches. These include failure to update software, inappropriate locations for data processing and failure to take appropriate steps when decommissioning software or services. Read the full article here.

Regulatory radar

EU: The Article 29 Working Party has published new guidance for the ecommerce sector on when to notify individuals about security breaches. Meanwhile, proposals on data and cyber security breach notification obligations under the draft **General Data Protection Regulation** and the **Network and Information Security Directive** continue to make their way through the Brussels legislature. In this article we summarise the latest state of play, and the impact of the recent EU elections on the process. Read the full article here.

Asia: Singapore's new data protection law comes into force on 2 July, hot on the heels of strict new financial services rules which will impose a one hour deadline for data breach notification.

US: we report on the Obama Administration's voluntary Cybersecurity Framework. Read the full article here.

Threat vectors

A selection of cyber threats and other stories that have made the headlines this month.

- China has decided to suspend its involvement in a cybersecurity working group with the US after being accused of commercial spying.
- A recent study found that 61 percent of energy firms view email as the biggest threat vector for cyber attacks via malware, and that hacktivists are seen as posing the biggest threat to energy companies.
- The United States is preparing to announce first-of-its-kind criminal charges on Monday 26 May against Chinese military officials accused of hacking into private-sector U.S. companies to gain trade secrets, a government official said.
- Seventeen men have been arrested in the UK as part of a worldwide crackdown on a malicious computer program, BlackShades.
- Reports of the Stoned Virus hitting the Bitcoin Blockchain prove to be false.
- Researchers have discovered previously unreported problems in SNMP on embedded devices where devices such as secondary market home routers and a popular enterprise-grade load balancer are leaking authentication details in plain text.
- More than a month after the world learned of the epic, headline-grabbing Heartbleed flaw, the severe OpenSSL vulnerability can still be found on hundreds of thousands of servers - and some other not-so-obvious spots due to an inconsistent industry-wide response.
- Last month Google offered refunds to users who bought a fake antivirus app from Google Play, but the scam seems to be catching on and security researchers have recently identified similar apps in both the Android and Windows Phone app stores.
- Buggy iTunes 11.2 update opened serious security hole on Apple Macs.
- An international operation led by the FBI has taken control of the GameOver Zeus botnet, a network of captured computers used to steal millions of dollars from individuals and small businesses around the world.

Key contacts

Blanca Escribano
Partner, Madrid
+34 91 187 1924
blanca.escribano@olswang.com

Sofía Fontanals
Senior Associate, Madrid
+34 91 187 1932
sofia.fontanals@olswang.com

Matthew Hunter
Associate, Singapore
+65 9827 8711
matthew.hunter@olswang.com

Ashley Hurst
Partner, London
+44 (0)20 7067 3486
ashley.hurst@olswang.com

Carsten Kociok
Senior Associate, Berlin
+49 30 700 171 119
carsten.kociok@olswang.com

Ross McKean
Partner, London
+44 (0)20 7067 3378
ross.mckean@olswang.com

Sylvie Rousseau
Partner, Brussels/Paris
+32 2 641 1272
sylvie.rousseau@olswang.com

Melanie Shefford
Associate, London
+44 (0)20 7067 3258
mel.shefford@olswang.com

Thibault Soyer
Avocat à la Cour, Paris
+33 1 70 91 87 75
thibault.soyer@olswang.com

Andreas Splittgerber
Partner, Munich
+49 89 206028 404
andreas.splittgerber@olswang.com

Elle Todd
Partner, Singapore
+65 9649 0449
elle.todd@olswang.com

Matthias Vierstraete
Advocaat, Brussels
+32 2 235 0301
matthias.vierstraete@olswang.com

OLSWANG

Berlin	+49 (0) 30 700 171 100
Brussels	+32 2 647 4772
London	+44 (0) 20 7067 3000
Madrid	+34 91 187 1920
Munich	+49 89 206 028 400
Paris	+33 17 091 8720
Thames Valley	+44 (0) 20 7067 3000
Singapore	+65 67208278

www.olswang.com

17578900-3