



Global Cyber Newsletter

December 2016



Notable Cyber Breaches

Australian Charity Breach



In Australia's largest security breach highly sensitive personal data of 550,000 blood donors of the [Australian Red Cross](#) was leaked when a file containing donor information was placed in an insecure computer environment and accessed by unauthorised persons. The breach is being investigated internally but the Red Cross believes that all copies of the data have now been deleted and the risk of data misuse is low.

UK National Health Service



All planned operations, outpatient appointments and diagnostic procedures were cancelled over a 3 day period at 3 UK hospitals following a [cyber-attack](#). Typically, the Trust would have 1,000 appointments per day. The Department of Health acknowledged that this was not the first attack on a UK hospital but declined to provide further details.

High Street Banking Breach



[Tesco Bank](#) faces an investigation by the UK regulator, the Financial Conduct Authority (FCA), when its customers' accounts had been subject to 'online criminal

activity'. This was an unprecedented attack on up to 40,000 customer current accounts in which money was taken from 20,000 accounts.

Information Commissioner's Office (ICO) will also be investigating. The bank has refunded £2.5m to 9,000 customers and claimed that personal data was not compromised.

YAHOO! Yahoo Breached Again

As discussed last quarter, Yahoo announced that [hackers](#) stole personal data on 500 million users back in 2014. The FBI is investigating and the European Article 29 Data Protection Working Party has requested full details from Yahoo.

On December 14th, Yahoo [announced](#) a second distinct breach had occurred in 2013 – this time exposing more than 1 billion user accounts. After this announcement, Verizon, which has been in lengthy negotiations to purchase Yahoo, is [reportedly exploring legal options](#) to renegotiate or exit the deal entirely.

'Mirai' Botnet Malware

A [major cyber-attack disrupts internet service across Europe and US](#) in what may have been the largest DDoS attack to date.

The Mirai malware principally targets vulnerable devices such as routers, digital records, webcams exploiting the use of default usernames and passwords.





In October the domain name system company Dyn was targeted resulting in extensive online disruption. The likes of Netflix, Twitter, Spotify, CNN and Amazon were impacted by the DDoS attack using the Mirai Botnet.

Chinese electronics manufacture Xiongmai recalled older versions of its webcams sold in the US after they were identified a contributor to the attack.

Two weeks later the same device was allegedly used to bring Liberia's internet infrastructure to a halt.

In Germany up to 900,000 Deutsche Telekom customers had broadband services cut following a suspected malware attack on a particular router. Internet access, phone connections and TV reception services were affected. It has been suggested that this failed attack was also linked to the broader Mirai attack.

In late November, certain routers supplied by Talk Talk and the Post Office were disrupted in the UK.

San Francisco Municipal Transportation Agency hacked



Just in time for the American Thanksgiving holiday, SFMTA was infected with ransomware on November 25th – a 100 bitcoin (~\$73,000 USD) ransom was demanded. The hacker also threatened to release 30GB of compromised data. SFMTA contacted the US Department of Homeland Security and the FBI, and isolated the systems being infected – by doing so, they opened the public transportation system up to fee use over the weekend to minimize disruption to passengers. Ultimately, no ransom was paid after the SFMTA was able to restore the system using a previous backup point.

Telecoms Industry Targeted




Following the 2015 attack on Talk Talk, another of the UK's largest telcom firms, Three had data of 130,000 customers compromised including names, phone numbers, addresses and dates of birth but no financial information. Entry was gained through an employee login and 3 people have been arrested. It is believed that the objective was theft by upgrading certain customers to new headsets and intercepting them.



 A possible compromise at one of the payment switch provider's systems is has threatened the security of 3.2m debit cards in India. More than 13m Rupees (US\$194,612) has been withdrawn through fraudulent transaction mainly in China and the US. All the major Indian banks are on alert. Whilst the financial cost is expected to be limited the reputational damage could be significant.

In response the insurance regulator, the IRDAI, will establish a comprehensive Cyber Security Framework with separate working groups for life and non-life sectors. Guidelines for the framework are expected to be issued in 2017.

Central Banks Targeted

 US\$31 million was stolen from banking client accounts of the Russia's Central Bank in a series of attacks in 2016. The attacks involved the faking of a client credentials. The bank confirmed that an attempted theft of 5 billion rubles was interrupted allowing it to redirect some of the funds.

US\$81m was stolen from the central bank of Bangladesh earlier this year when a bank official's computer was used by unidentified hackers to make payments via Swift.




Another Breach for BCBS

Blue Cross / Blue Shield reported another breach – at least the third – in recent years, in late November. Although breach is comparatively small (~170,000 records) and results from a printing error rather than malicious action, the fact that BCBS is a “repeat offender” may draw the attention of regulators.

Regulatory & Legislative Update

'Snoopers' Charter' becomes law in the UK

 The highly controversial Investigatory Powers Bill received Royal Assent in November and will become law in the UK. The new legislation will provide security and law enforcement agencies with unprecedented powers of surveillance. The principal aim is national security and disruption of terrorist attacks. Notably, the new Act will require internet service providers (ISPs) to store browsing records of users for 12 months. Police and security services will have powers of interception, equipment interference or bulk communications acquisition data in bulk. The most intrusive powers will require a warrant from the Secretary of State and approval by a senior judge.



Recent Regulatory Penalties

Record UK Fine

The UK [Information Commissioner's Office](#) has fined telecommunications provider Talk Talk £400,000 for a cyber-attack that exploited vulnerabilities in three of its webpages. The webpages were inherited when Talk Talk acquired Tiscali in 2009. The attacker performed a SQL injection attack exposing the personal data of 156,959 customers including bank account numbers and sort codes. A fix for this known vulnerability was available in 2012.

The ICO exercised its powers under the Data Protection Act 1998 (DPA) which will be replaced by the European General Data Protection Regulation (GDPR). Under DPA the ICO has the power to issue fines up to £500,000. GDPR will give European regulators significantly increased scope to fine organizations up to 4% of worldwide turnover or €20m.

Previous significant fines include the Brighton and Sussex University Hospital NHS Trust which was fined £375,000 when hard drives containing patient data had been sold on eBay by a contractor it had employed to destroy them. In 2013, the ICO fined Sony £250,000 after hackers stole customer data stored on its PlayStation network.

ICO monetary penalties 1Q2016:

Blackpool Teaching Hospital NHS Foundation Trust	£ 185,000
Chelsea and Westminster Hospital NHS Foundation Trust	£ 180,000
Chief Constable of Dyfed Powys police	£ 150,000
Chief Constable of Kent police	£ 80,000

Source: ICO 1Q2016

U.S. Dept. of Health and Human Services Steps Up Fines

In a year that has [already seen the HHS stepping up regulatory actions](#) against violators of the HIPAA regulations, the fourth quarter saw two more significant settlements: [UMass](#) entered a corrective action plan and paid a \$650k fine – which reportedly would have been larger had the University not operated at a financial loss in 2015; and [St. Joseph Health](#) entered a corrective action plan and paid a ~\$2.14M penalty.

Singapore Fines



As reported in the 2Q update, the Singapore Data Protection

Commission (PDPC) [fined](#) K Box Entertainment, the Karaoke outlet operator, and its IT vendor S\$50,000 and S\$10,000 respectively. The personal data of 317,000 members were leaked in 2013. The recently released reasoning behind the fine was the failure to implement proper and adequate protective measures to secure its IT system resulting in the unauthorized disclosure of personal data. In addition, there were issues



with weak passwords and sending customer data by unencrypted mail.

Other PDPC 4Q Penalties

PDPC penalties 4Q2016:

Toh-Shi Printing Singapore	\$ 25,000
Fu Kwee Kitchen Catering & Pixart	\$ 5,000
Smiling Orchid	\$ 3,000
GMM Technoworld	\$ 3,000

Source: PDPC

New Chinese law troubles international business



Although this new law largely codifies existing Chinese practices in the cybersecurity arena, it is troublesome for international business groups as the definition of “critical information infrastructure” is very broad – thus requiring Chinese government access to code and technologies of foreign corporations. The law goes into effect in June 2017.

Global Cyber Security

U.K. Government Invests in Cyber Security

The UK Government has announced that it plans to spend £1.9bn on cyber security over 5 years. The spend will enlarge the specialist police units that tackle organized online gangs, the education and training of cyber security

experts with the capability to retaliate in kind against hostile foreign actors.

U.S. Commission on Enhancing National Cyber Security Releases Report

After conducting a nine-month study of America’s cybersecurity problems, the commission created by President Obama released the results in an extensive report. It contains a number of detailed plans: from requiring a higher level of baked-in security in IoT consumer devices to prevent botnet attacks to reorganising responsibility for cybersecurity among U.S. federal agencies. However given the timing, it will be President-Elect Donald Trump, who takes office January 20, 2017, who makes the decision whether to act on these recommendations.

U.S. and U.K. Officials Face Russian Hacking

Reports now issued from both sides of the Atlantic, that the U.K and the U.S. are simultaneously facing a variety of hacking efforts, purportedly by the Russian government. As purported state-sponsored hacking on this level is new diplomatic ground, the appropriate response is unknown.



Cyber Litigation News

Legal Challenge to Privacy Shield

Privacy Shield, the new mechanism for transferring data between the EU and US and became operational in August is to face a legal challenge. Irish and French groups have asked the European Union's General Court to annul the framework. Over 500 companies have already signed up to Privacy Shield including Facebook, Google and Microsoft.

Privacy Shield was the successor to Safe Harbor which was successfully invalidated in an earlier challenge through the European Courts.

When Dynamic IP Addresses = Personal Data



In (Patrick Breyer v Bundesrepublik Deutschland), the Court of Justice

of the European Union (CJEU) was asked whether dynamic addresses gathered from visitors to websites constituted personal data under the EU Data Protection Directive 95/46/EC.

A dynamic IP address is an IP address which can change at each new connection to the internet. The website operator cannot identify the user without additional data.

The case originated in Germany where Mr. Breyer challenged the storage of dynamic IP addresses by state-owned websites. These publically accessible websites stored IP addresses of visitors to the website for the purposes preventing cyber attacks and bringing criminal prosecutions.

Under the directive, an identifiable person is one who can be identified directly or indirectly. Mr. Breyer could be indirectly identified by the combination of his IP address and account data held by his Internet Service Provider (ISP).

The CJEU ruled that dynamic IP addresses may constitute personal data if a third party e.g. ISP held additional information (obtained lawfully) that could be used to identify the individual.

The decision is significant because it means that the collection and subsequent processing of IP addresses may be subject to EU data protection laws.

U.S. – Delaware Court Ruling Applicable to Cyber Arena




In Reiter v. Fairbank, C.A. (No. 11693-CB; Del. Ch. Oct. 18, 2016), the court offers guidance on how directors and officers must act in order to avoid bad faith in their oversight of the corporation's compliance in a



risky and heavily regulated environment. Although the case itself concerns money-laundering, the parallels to corporate governance of cyber security are clear, and can be interpreted as supporting the decisions in the *Wyndam* and *Target* derivative actions. In reviewing such actions, courts will focus on actual legal compliance, presence of good faith systemic controls, and good faith, amongst others.

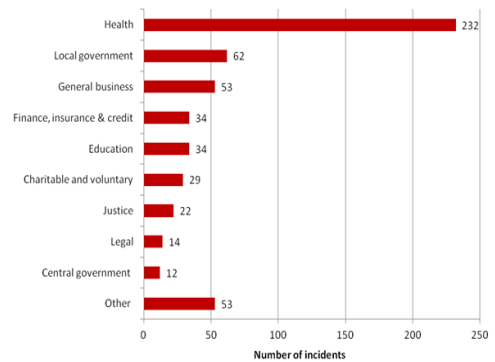
Cyber Studies

 The cyber specialist, NetDiligence has released its 2016 cyber claims study. The study is based on a survey of actual data breach insurance claims principally in the US. According to the study, the most expensive breaches occurred in Financial Services which also exposed the largest number of records. Health being the sector most frequently breached followed by Financial services. There was insider involvement in 30% of the cases surveyed.

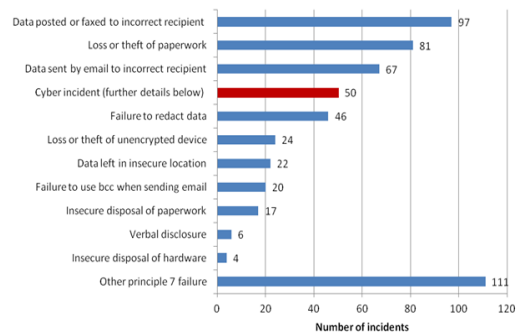
 The Information Commissioner's Office has released a report on Data Security Trends. The tables below represents 1Q data security incidents by sector.

Not dissimilar to the NetDiligence study, the Health sector leads the way in terms of number of breaches and Finance, Insurance and Credit sector saw incidents increase by 36% on the prior period. Incidents linked to human error represent the majority breaches.

Data security incidents by sector



Data security incidents by type



UK Government Cyber Survey

UK Government sponsored Cyber breach survey of over 1,000 UK business revealed that cyber security is high priority for nearly 70% of businesses. However, just over 51% have taken recommended action to identify cyber risk. A quarter of the business surveyed detected one or more cyber breaches in the last 12 months.



This was significantly higher in medium to large firms which were 51% and 65% respectively. 25% experienced a breach at least once a month.

The most costly breach in the survey was £3m with the average breach cost to large business being £36,500. The average cost was £3,480 over the last 12 months. 68% of the breaches/attacks were virus/spyware/malware related with 32% linked to the impersonation of the organisation.



McAfee Labs Threats Report

McAfee labs has released their [Threats Report](#) for December 2016, examining current threats and looking forward to 2017, predicting what types of cyber threats will become more / less common.



The Geneva Association

Key Questions on Cyber Risk

International insurance industry think tank The Geneva Association released their report entitled "[Ten Key Questions on Cyber Risk and Cyber Risk Insurance](#)" in December 2016, delving into current knowledge and practices in the Cyber Insurance community.



Contacts

Peter Cridland

Assistant Vice President

T: 1 212 365 2032

E: pcridland@transre.com**Kara Owens**

Global Head of Cyber Risk

T: 1 212 365 2340

E: kowens@transre.com**Lauren Markowski**

Cyber Risk Underwriter

T: 1 212 365 2301

E: lmarkowski@transre.com**Rhett Hewitt**

Cyber Risk Underwriter

T: 44 (0)20 7204 8676

E: rhewitt@transre.com**Calum Kennedy**

Vice President Claims

T: 44 (0)20 7204 8645

E: ckennedy@transre.com

To receive future editions of the TransRe Cyber Newsletter, please [CLICK HERE](#) and include your name, title and organization in the body of the email.

Disclaimer: The material and any conclusions contained in this document are for information purposes only and the authors offer no guarantee for the completeness of its contents. The statements in this document may provide current expectations of future events based on certain assumptions. These statements involve known and unknown risks, uncertainties and other factors which are not exhaustive. The authors of this document undertake no obligation to publicly revise or update any statements, whether as a result of new information, future events or otherwise and in no event shall TransRe or any of its affiliates or employees be liable for any damage and financial loss arising in connection with the use of the information relating to this document. Although TransRe makes reasonable efforts to obtain reliable content from third parties, TransRe does not guarantee the accuracy of or endorse the views or opinions given by any third party. This document may point to websites or other documents, however TransRe does not endorse or take responsibility for the content on such websites or other documents.

