Global Cyber Newsletter

March 2017

TransRe

We value Cyber risk.

Notable Cyber Breaches

Asia Pacific

Shamoon Variant

Public and private sector organizations in Saudi Arabia have been targeted with the Shamoon virus. The virus is believed to be a variant of a virus used in a ransomware attack against the Kingdom in 2012. The 2012 attack was considered to be state sponsored and resulted in the partial wiping/destruction of up to 35,000 computers. The full extent of the damage in the current instance is unknown.

Indian ATMs attacked

India's banking system suffered a massive breach between May and July 2016 compromising the debit card data (including Visa and Mastercard) of 3.2 million customers. The malware attack targeted ATM terminals of Yes Bank which were managed by Hitachi Payment Services. The attack wasn't discovered until September. A number of other banks including ICICI Bank, HDFC Bank and AXIS Bank confirmed that customer card accounts had possibly been breached.

Taiwan DDoS Ransom

Several securities companies in Taiwan were threatened with Distributed Denial of Service (DDoS) attacks by a group making ransom demands. Bitcoin payments of TWD 300,000 were demanded. No payments were made and reported attacks suggested only minor disruption.

Singapore Ministry of Defense Hacked

In what is believed to be a targeted attack, the personal data of 850 Singapore servicemen and employees was stolen. Whilst personal ID numbers, phone numbers and dates of birth were taken, this didn't include classified data..

Europe

Another UK Banking attack

Lloyds Banking Group suffered a two day DDoS attack which temporarily stopped customers of Lloyds, Bank of Scotland and Halifax from accessing their accounts online. It is understood that no money or data was stolen.

Hotel Lock Down

Hackers seized control of the electronic key system in a 4 star Austrian Hotel. The ransomware attack locked guests out of rooms. The hotel paid a ransom demand reported to be€1,500 in Bitcoins.

United States

Yahoo – Verizon Update

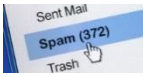
After multiple large-scale breaches reported in 2016, speculation was rampant that Yahoo's purchase by Verizon was in jeopardy. In February, the companies jointly revealed that the purchase will go forward at $4.48B - a $350M reduction in purchase price. The US Securities and Exchange Commission (SEC) is understood to have opened an investigation into whether the data breaches should have been reported to investors sooner. Under the terms of the deal, Yahoo will bear sole responsibility for any liabilities associated with the SEC investigation and any shareholder lawsuits. In related news, the U.S. Department of Justice indicted four individuals connected to one of the Yahoo breaches, including two officers in Russia's intelligence agency, the FSB.

Amazon Servers Falter

Amazon servers suffered a failure affecting an unknown number of websites including Medium, Slack, Trello. Affected systems were part of an Amazon Web Service called Amazon Simple Storage Service (S3), which stores data for retreival by websites when needed. Although revealed to have been caused by internal error rather than 3rd party action, the 4-hour downtime coincided with the UK's AWSome Day. S&P 500 companies were reported to have lost $150m. Contingent business interruption may trigger cyber policies in excess of waiting times.

Connected Toys Reveal Private Information

CloudPets, made by Spiral Toys, are wifi-connected stuffed animals that allow family members to record messages to be played through the stuffed animal to a child (or alternatively, for the child to record audio). It was revealed in February that those audio files were being stored online and were not properly secured, exposing those personal messages to anyone interested in snooping. It appears at least 820k users were part of the data exposed.



River City Media reveals data on 1.4 Billion accounts

Notorious SPAM operation River City Media was found to have left 1.4 email addresses, linked to real names, IP and physical addresses unprotected on the internet after an error in their backup system.

Regulatory & Legislative Update

Asia Pacific

Cyber Regulations Proposed in India

The Insurance Regulatory and Development Authority of India has proposed a requirement for all re/insurers to take action to protect the data they store or face monetary penalties.

Europe

National Security Verses Privacy

The highly controversial Investigatory Powers Act which was passed into law in the UK in November last year has been held illegal by the European Court of Justice. The new legislation granted security services with powers for the bulk collection of personal communications in addition to powers to hack and bug computers and phones. The court's principal objections were that access to such data must be targeted and restricted to the purpose of preventing and detecting serious crime. It also ruled that the police and public bodies should not be allowed to authorise their own access to this data.

The ruling draws parallels with concerns that the same court had when invalidating Safe Harbor (*Schrems v Data Protection Commissioner*). Safe Harbor was the voluntary initiative which allowed US organizations to self-certify that data was processed in accordance with the EU data protection directive. Concerns were heightened by the revelations of Edward Snowden regarding widespread monitoring of data by US security agencies.

Penalties Become Personal

From Spring 2017, directors of firms in the UK found to be making nuisance calls can be personally fined up to £500,000 by the ICO. This is to prevent directors declaring the company bankrupt as a means of avoiding corporate penalties.

Asia Pacific

Recent Regulatory Penalties

PDPC Enforcement

Entity or Individual	Monetary Penalty
Propnex Reality	SGD 10,000
JP Pepperdine	SGD 10,000

Source: Person Data Protection Commission Singapore

Europe

Multinational general insurance company, Royal & Sun Alliance, received a monetary penalty notice of £150,000 from the ICO following the theft of a portable 'Network Attached Storage' device in 2015 from a data server room. The device contained 59,592 customer names, addresses, bank

accounts and sort code numbers. It also held credit card details of 20,000 customers although expiry dates and CVV numbers were not held on the device. The device was password protected but not encrypted. The ICO's principal concerns related to the failure of appropriate technical & organizational measures relating to the security of the server room to prevent unauthorized access.

Health Care provider, HCA International was fined £200,000 by the ICO for routinely sending unencrypted audio recordings of patient consultations to a data processor in India. The data processor used an unsecured FTP server to store the recordings. Transcripts of consultations that took place in March/April 2015 became accessible via an internet search engine.

Regulator Self-Reports

The ICO has upheld 14 complaints against its own office in 4 years according to information obtained under a Freedom of Information Request. Out of 40 complaints against the ICO since 2013, seven resulted in orders to take action.

ICO Enforcement

Entity or Individual		Monetary Penalty
HCA International	£	200,000
Royal & Sun Alliance PLC	£	150,000
LAD Media Ltd	£	50,000
IT Protect Ltd	£	40,000
The Data Supply Company	£	20,000
Rebecca Gray	£	200

Source: Information Commissioner's Office

United States

New York State Finalizes Cybersecurity Rule

The New York State Department of Financial Services issued its final regulation – effective March 1, 2017 – requiring all covered entities in the state have a cybersecurity program that meets new, heightened standards. Notably, the rule requires: all non-public data be encrypted, restricted access to systems and data, "timely" destruction of non-public information, and the designation of a CISO to oversee the program, which must be re-certified annually. Covered entities have a year and a half to comply.

Trump Administration Cancels Signing of Cybersecurity Executive Order

The Trump administration scheduled and then cancelled the signing of an Executive Order on cybersecurity. A draft of that Order has been

published by several news outlets. It is unknown when, or in what form, any executive action on cybersecurity will occur – but the Trump administration has circulated a third draft.

U.S. Dept. of Health and Human Services Continues Fines

As reported last quarter, the Department of Health and Human Services, which enforces HIPAA, is continuing to investigate breaches and issue fines at a high rate. In January, Presence Health paid a $475k fine for failure to timely notify the Department of a breach, and MAPFRE Life Insurance Company of Puerto Rico paid a $2.2M settlement. In February, Florida's Memorial Health Systems entered into a $5.5M settlement agreement, and Children's Medical Center of Dallas paid a $3.2M penalty for HIPAA violations.

HHS – Office of Civil Rights "Wall of Shame" Update

The Department of Health and Human Services – Office of Civil Rights is also charged by the HITECH Act to publish an ongoing list of breaches affecting 500 or more individuals. 56 such breaches have been posted in 2017.

Congress Votes to Repeal Privacy Rules

In late March, the U.S. Senate voted to repeal a Federal Communications Commission (FCC) rule requiring internet service providers (ISP) to safeguard the privacy of their customers. On the 28th, the House of Representatives followed suit, and sent the bill to the President for signature. The repeal allows ISPs to catalog and sell data about the web surfing habits of their individual customers. The President is expected to sign the bill

Special Guest Column

H|B|S HALL BOOTH SMITH, P.C.
ATTORNEYS AT LAW
Serving to Achieve Excellence

5 Things You Can Tell Your Clients To Do Right Now To Reduce Their Data Breach Risk....And They Hardly Cost Anything!

By Richard Sheinis

Having handled over 100 data breaches I have seen a few trends. Sometimes people get so caught up in the sophisticated breaches like Target or Sony, that they don't remember to do the easy things that can reduce the likelihood of being a breach victim, or reducing the damages if they are a victim. So here are 5 things you can tell your clients in almost any industry to reduce their data breach risk without even spending much money:

1. **If You Do Not Need the Data, Don't Save It**

Having excess data or personal information just makes the damages worse if you are breached. Do you want to notify 100,000 people that their personal information was stolen, or would you rather notify 1,000? Have a good data retention policy so that data is deleted when it is no longer needed. If you are in an industry, such as health care, where various laws require that you retain data for a certain period of time, or if you are a data pack rat and hate to throw anything away, but you do not need the data for day-to-day operations, get it out of your computer system, and store it offline. If the data is not in your computer system, and is not accessible from the internet, it is much safer.

2. **Provide Security Awareness Training**

Most hackers depend on someone in the target company "allowing" them into the computer system. Phishing e-mails and social engineering scams depend on someone opening a phishing e-mail, clicking on an attachment, or being tricked into revealing login credentials, in order for the hacker to gain access to the system. Spend an hour or two teaching your employees about these scams, and how to recognize them so they do not mistakenly open the door for the hacker.

3. **Get Breach Detection Software**

Okay, this one might cost a few bucks depending on the size of the company, but I think it is worth it. Once a hacker gains entry to a computer system, they might hang around awhile. They don't always take the data and run. They may inject malware to "watch" your computer system, look around for passwords and other sensitive data, and then even take steps to cover their tracks. I have seen studies that state the average time from a breach occurring until the time it is discovered is over 200 days. A lot of bad things can happen in 200 days! On the other hand, I have seen a number of companies saved because their system alerted them to the presence of malware, and they were able to stop the hacker before any damage was done.

4. **Strong and Secret Passwords**

A "brute force" attack is when a hacker guesses a password to gain access to a network. There are thousands of hackers that sit at computers all day doing nothing but guessing passwords. Many people still use their child's first name or the name of their favorite sports team, or their college, as their password. All of which is frequently on a person's Facebook page, or some other social media account. Also, don't let employees put their password on a sticky note on their computer monitor or under their keyboard. Strong passwords are too hard to remember? Use a free password manager like OnePass or DashLane.

5. **Restrict Access**

Does everyone in the organization require access to every bit of data or personal information in the computer system? If they do not, institute an access management system so people only have access to the data they need to do their job. Or if employees only need limited access to data, restrict their acces s so they can view the data, but they cannot write over it, copy it, download it, or transmit it. Access management helps avoid insider theft of data, or if an employee's password is compromised, the hacker's access is limited to the same access rights of the employee.

There you have it, five ways to reduce data breach risk, and how much did it cost?

About the author: *Richard Sheinis has litigated in federal and state courts for thirty years. He has been the first chair for approximately 175 jury trials. His clients have included health care professionals and institutions, technology companies and global business entities. Mr. Sheinis takes advantage of his litigation background to work with businesses in the areas of data privacy and security, employment and technology. He works with a wide variety of companies from small technology businesses to publicly traded companies with a global footprint.*

Global Cyber Security

United States

United States Central Intelligence Agency Suffers WikiLeaks Breach

The C.I.A., America's foreign intelligence service has suffered what is believed to be a leak from an insider, who provided a trove of documents to Wikileaks. The documents detail hacking tools used by the Agency to collect information through hacking individual phones or other connected devices, inciting fear that these tools can now be used by any hacker.

Factories infected with Malware

Cybersecurity firm Dragos has revealed that at least 10 industrial plants worldwide have been infected with malware disguised as Siemens software. Although no damage was reported, the incident raises the specter of physical damage caused by a cyberattack, as in the widely-reported German steel factory incident in late 2015.

Litigation News

Europe

Defamation & Data Protection Not Mutually Exclusive

The English Court of Appeal has ruled that a claim for defamation does not preclude a claim being pursued for breach of data protection laws. Prince Moulay Hicham of Morocco claimed that he had been defamed by publisher, Elaph Publishing in an article in October 2014 and that this also constituted a breach of the Data Protection Act by processing inaccurate personal data.

United States

Home Depot Settles with Banks

Home Depot has reached agreements to settle lawsuits with banks and credit unions following its 2014 data breach which exposed more than 50 million customer payment cards. The $25m settlement resolves 25 class actions from 50 financial institutions. The financial institutions alleged lax security practices led to the breach.

Home Depot previously paid $19.5m to compensate US consumers. The retailer reported in its third-quarter earnings that it had spent $288m on data-breach related expenses of which, $100m will be recouped from insurance.

Increase in Cyber Litigation on the Horizon

2016 saw several important legal decisions in the Cyber arena that are now being used as guides for ongoing litigation as well as for how coverages are drafted. Many industry experts believe 2017 will see a significant increase in cyber litigation. With increases in regulation – as discussed above – and significant legal issues still subject to conflict between courts around the country, 2017 is poised to set a new high-water-mark for cyber litigation.

Arby's Hit with Class-Action Lawsuit

Fast food company Arby's has been named in a class-action lawsuit related to a breach of their POS system. The suit is being brought by financial institutions to recoup the costs associated with reissueing debit and credit cards to the affected consumers.

Cyber Studies/Trends

The UK's National Cyber Security Management Centre has warned of a big bank failure in 2017 resulting from a cyber breach. According to the Financial Conduct Authority (FCA) more than 75 cyber attacks were reported in the first 9 months of 2016 compared to 5 in the whole of 2014.

Quiet 4Q for Attacks

Akamai, the US content delivery network and cloud service provider reported a surprisingly quiet 4Q period for web attacks. The Mirai botnet continues to be one of the largest threats. The public release of the Mirai source code has led to a series of copycat botnets.

Advisen Compares Cyber Regs

Advisen offers commentary comparing current and pending U.S. and U.K. cyber regulations as governments participation in the cyber space evolves and intensifies in 2017.

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.