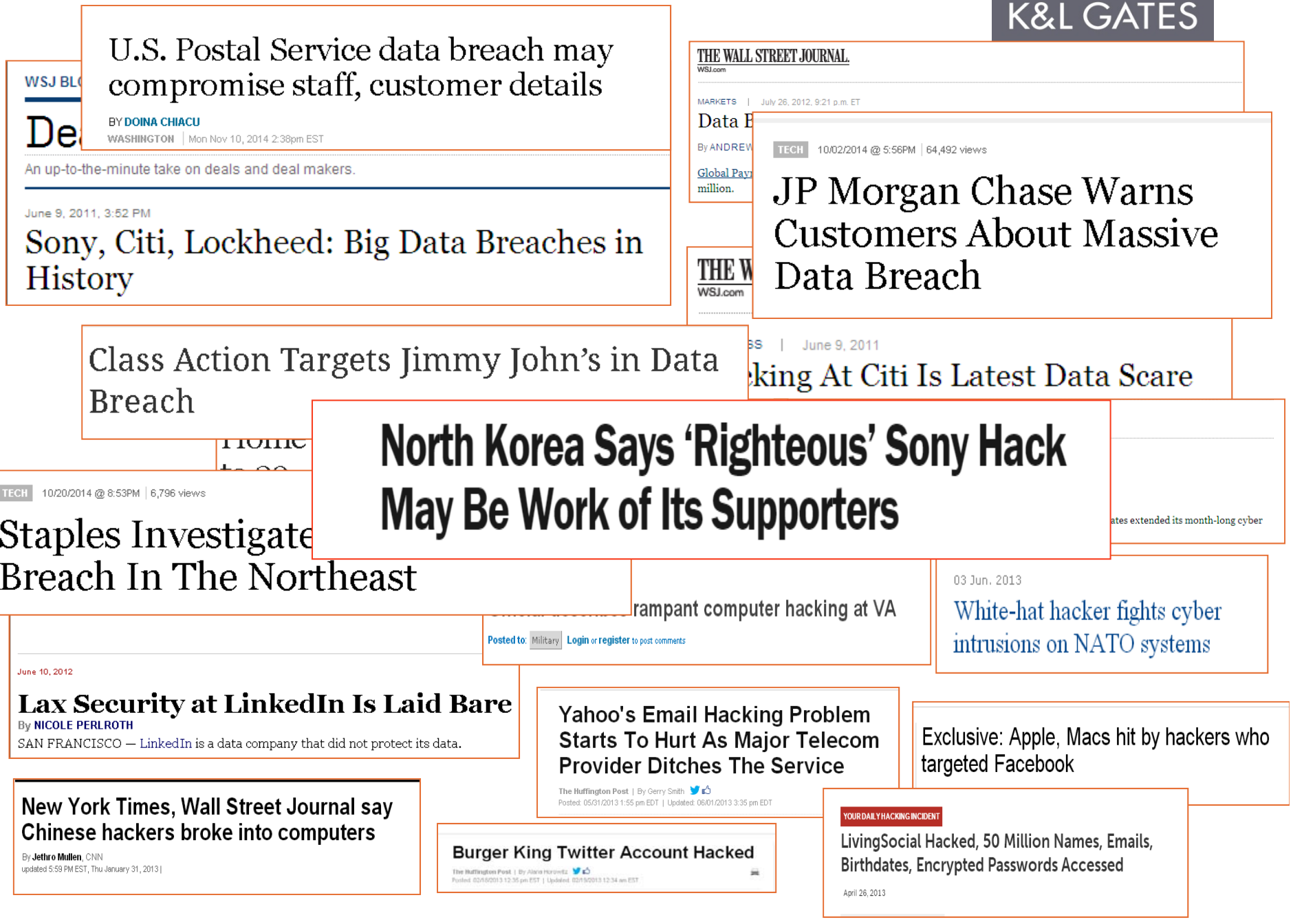
K&L GATES

10 December, 2014

Identifying Cyber Risks and How they Impact Your Business

David Bateman, Partner, K&L Gates, Seattle

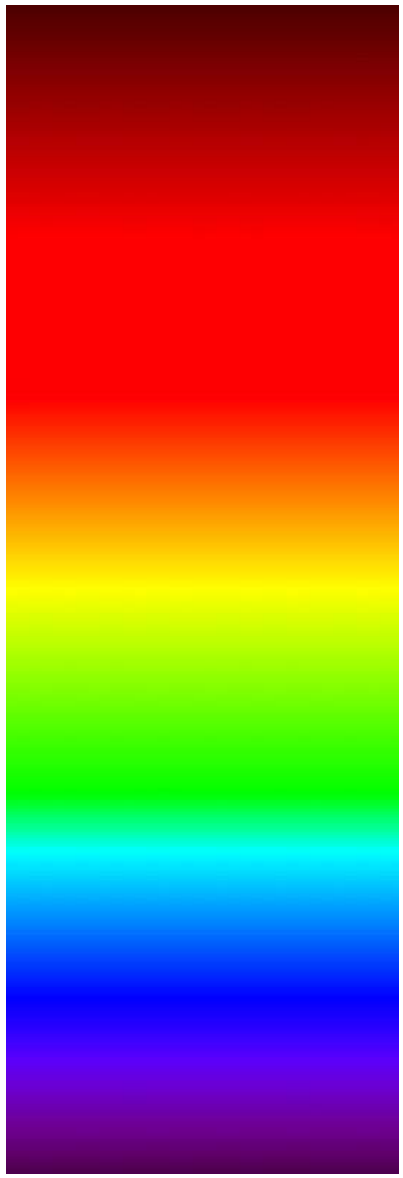
Sasi-Kanth Mallela, Special Counsel, K&L Gates, London


U.S. Postal Service data breach may compromise staff, customer details
BY DOINA CHIACU
WASHINGTON | Mon Nov 10, 2014 2:38pm EST
WSJ BL
De
An up-to-the-minute take on deals and deal makers.
June 9, 2011, 3:52 PM
Sony, Citi, Lockheed: Big Data Breaches in History
THE WALL STREET JOURNAL.
WSJ.com
MARKETS | July 26, 2012, 9:21 p.m. ET
Data B
By ANDREW
Global Pay
million.
TECH 10/02/2014 @ 5:56PM | 64,492 views
JP Morgan Chase Warns Customers About Massive Data Breach
THE W
WSJ.com
SS | June 9, 2011
king At Citi Is Latest Data Scare
Class Action Targets Jimmy John's in Data Breach
North Korea Says 'Righteous' Sony Hack May Be Work of Its Supporters
TECH 10/20/2014 @ 8:53PM | 6,796 views
Staples Investigate
Breach In The Northeast
ates extended its month-long cyber
rampant computer hacking at VA
Posted to: Military Login or register to post comments
03 Jun, 2013
White-hat hacker fights cyber intrusions on NATO systems
June 10, 2012
Lax Security at LinkedIn Is Laid Bare
By NICOLE PERLROTH
SAN FRANCISCO — LinkedIn is a data company that did not protect its data.
Yahoo's Email Hacking Problem Starts To Hurt As Major Telecom Provider Ditches The Service
The Huffington Post | By Gerry Smith
Posted: 05/31/2013 1:55 pm EDT | Updated: 06/01/2013 3:35 pm EDT
Exclusive: Apple, Macs hit by hackers who targeted Facebook
New York Times, Wall Street Journal say Chinese hackers broke into computers
By Jethro Mullen, CNN
updated 5:59 PM EST, Thu January 31, 2013
Burger King Twitter Account Hacked
YOUR DAILY HACKING INCIDENT
LivingSocial Hacked, 50 Million Names, Emails, Birthdates, Encrypted Passwords Accessed
April 26, 2013

K&L GATES

The Spectrum of Cyber Attacks

- Advanced Persistent Threats (“APT”)
- Cybercriminals, Exploits and Malware
- Denial of Service attacks (“DDoS”)
- Domain name hijacking
- Corporate impersonation and Phishing
- Employee mobility and disgruntled employees
- Lost or stolen laptops and mobile devices
- Inadequate security and systems: third-party vendors



Advanced Persistent Threats

- targeted, persistent, evasive and advanced
- nation state sponsored

P.L.A. Unit 61398
"Comment Crew"

Advanced Persistent Threats

- United States Cyber Command and director of the National Security Agency, Gen. Keith B. Alexander, has said the attacks have resulted in the "greatest transfer of wealth in history."

U.S. Blames China's Military Directly for Cyberattacks

By DAVID E. SANGER
Published: May 6, 2013 | 264 Comments

WASHINGTON — The Obama administration on Monday explicitly accused China's military of mounting attacks on American government computer systems and defense contractors, saying one motive could be to map "military capabilities that could be exploited during a crisis."

FACEBOOK
TWITTER
GOOGLE+
SAVE
E-MAIL

U.S. and China Agree to Hold Regular Talks on Hacking

By DAVID E. SANGER and MARK LANDLER
Published: June 1, 2013

WASHINGTON — The United States and China have agreed to hold regular, high-level talks on how to set standards of behavior for cybersecurity and commercial espionage, the first diplomatic effort to defuse the tensions over what the United States says is a daily barrage of computer break-ins and theft of corporate and government secrets.

FACEBOOK
TWITTER
GOOGLE+
SAVE
E-MAIL

Source: New York Times, June 1, 2013.

K&L GATES

Advanced Persistent Threats

- The Director-General of MI5 warned that one London business suffered £800 million in losses following an attack
- The UK's National Security Council has judged that the four highest priority risks are currently those arising from:
  - International terrorism
  - **Cyber attack**
  - International military crises and
  - Major accidents or natural hazards**

*Source: Cyber crime a global threat, MI5 head warns (2012) http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9354373/Cyber-crime-a-global-threat-MI5-head-warns.html

** Source: A Strong Britain in an Age of Uncertainty: The National Security Strategy (October 2010)

K&L GATES

Advanced Persistent Threats

- A survey by anti-virus specialists Kaspersky found that cyber security measures taken by UK businesses were “woefully inadequate”
- Only 25% of IT specialists thought that their company was completely protected from cyber threats - although can there ever be complete protection?
- When questioned, 33% of IT managers did not know anything about the common cyber threats that have been targeting corporates

*Source: BCS – The Chartered Institute for IT - http://www.bcs.org/content/conWebDoc/49048

Advanced Persistent Threats

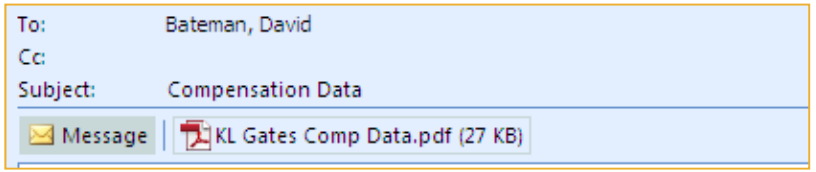
- Penetration:
  - 67% of organizations admit that their current security activities are insufficient to stop a targeted attack.*
- Duration:
  - average = 356 days**
- Discovery: External Alerts
  - 55 percent are not even aware of intrusions*

**Source: Mandiant, “APT1, Exposing One of China’s Cyber Espionage Units”

*Source: Trend Micro, USA. http://www.trendmicro.com/us/enterprise/challenges/advance-targeted-attacks/index.html

Advanced Persistent Threats: Penetration

- Spear Phishing



- Watering Hole Attack

  rely on insecurity of frequently visited websites

- Infected Thumb Drive

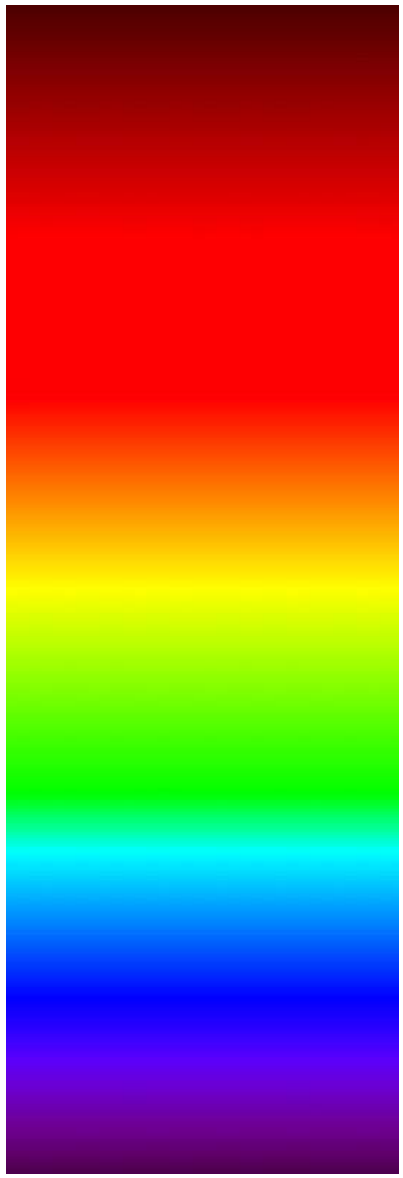
**Source: Mandiant, "APT1, Exposing One of China's Cyber Espionage Units"

*Source: Trend Micro, USA. http://www.trendmicro.com/us/enterprise/challenges/advance-targeted-attacks/index.html

K&L GATES

The Spectrum of Cyber Attacks

- Advanced Persistent Threats (“APT”)
- Cybercriminals, Exploits and Malware
- Denial of Service attacks (“DDoS”)
- Domain name hijacking
- Corporate impersonation and Phishing
- Employee mobility and disgruntled employees
- Lost or stolen laptops and mobile devices
- Inadequate security and systems: third-party vendors

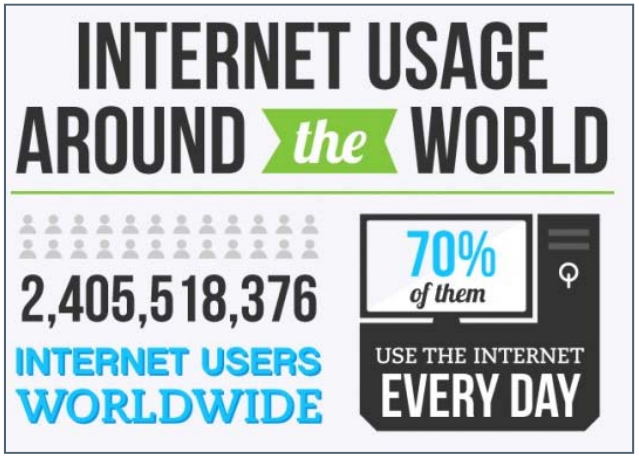


Cybercriminals, Exploits and Malware

TECHNOLOGY

Russian Hackers Amass Over a Billion Internet Passwords

By NICOLE PERLROTH and DAVID GELLES AUG. 5, 2014



Cybercriminals, Exploits and Malware

- 60,000 known software vulnerabilities
- 23 new zero-day exploits in 2014

Shellshock Bug May Be Even Bigger Than Heartbleed: What You Need to Know

Sep 26, 2014, 1:18 PM ET

- Risk = threat + vulnerability

Cybercriminals, Exploits and Malware

- Ransomware

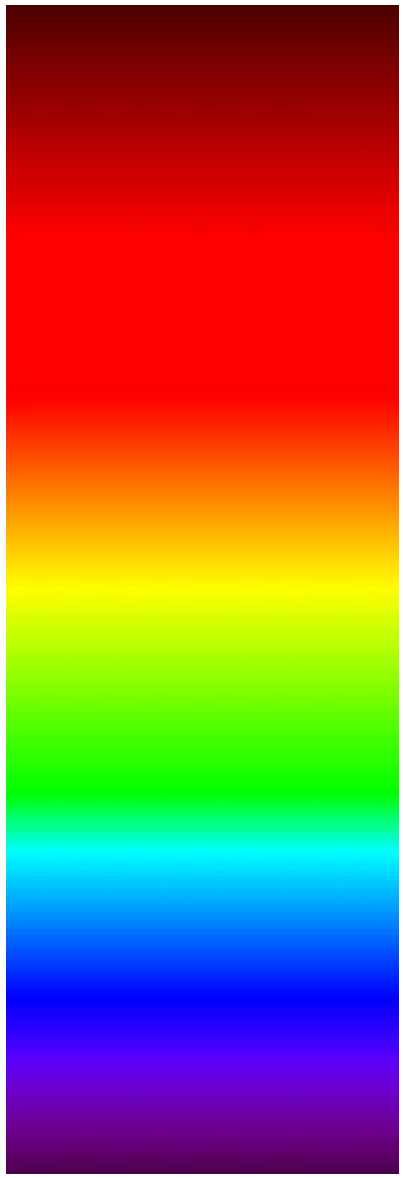
UK Law Enforcement

CryptoLocker

K&L GATES

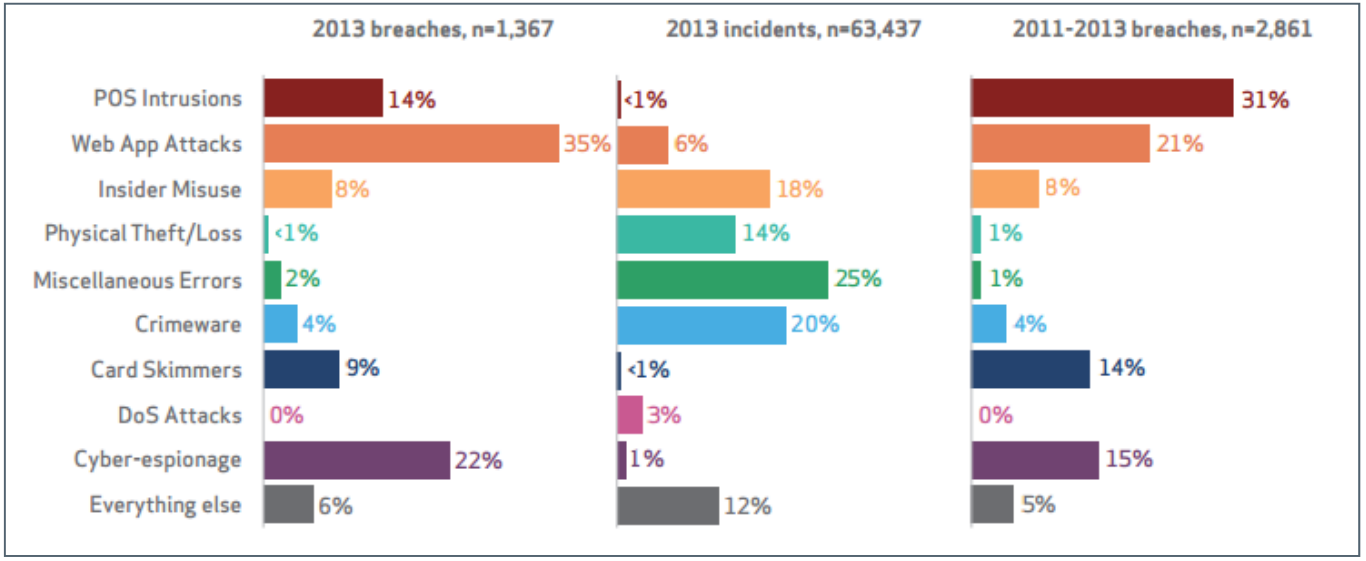
The Spectrum of Cyber Attacks

- Advanced Persistent Threats (“APT”)
- Cybercriminals, Exploits and Malware
- Denial of Service attacks (“DDoS”)
- Domain name hijacking
- Corporate impersonation and Phishing
- Employee mobility and disgruntled employees
- Lost or stolen laptops and mobile devices
- Inadequate security and systems: third-party vendors



Inadequate security and systems: third-party vendors

- Vendors with client data
- Vendors with password access
- Vendors with direct system integration
  - Point-of-sale



Inadequate security and systems: third-party vendors

K&L GATES

Cybercriminals, Exploits and Malware

- In the UK, a government report found that the cost of cyber security breaches nearly doubled in 2013
- For large organisations the worst breaches cost between £600,000 and £1.158 million (up from £450-£850k a year ago)

*Source: UK Government press release, 29 April 2014 https://www.gov.uk/government/news/cost-of-business-cyber-security-breaches-almost-double

K&L GATES

Cybercriminals, Exploits and Malware

Cost Per Record: $158
Notification Costs: $509,000
Post-Breach Costs: $1.6M
Business Loss: $3.3M

*Source: Symantec Internet Security Trend Report 2014

Dangers of New and Emerging Risks

Cloud Computing Risks

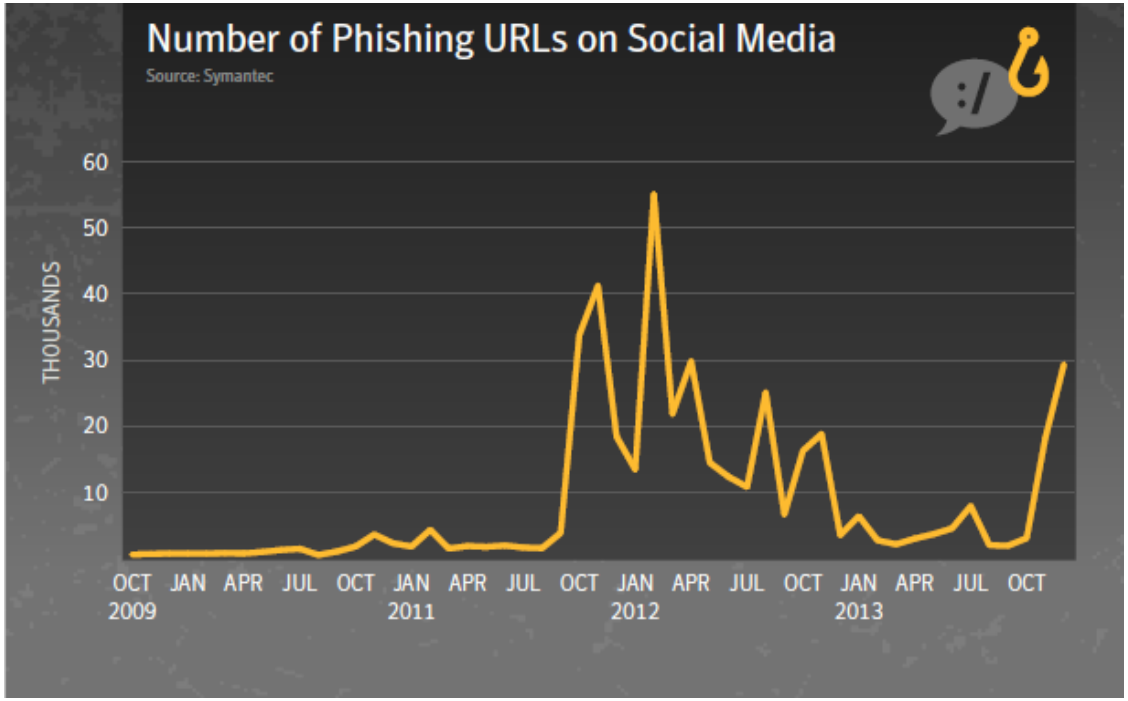
- Exporting security function and control
- Geographical uncertainty creates exposure to civil and criminal legal standards
- Risk of collateral damage

Mobile Device Risks

- 52% of mobile users store sensitive files online
- 24% of mobile users store work and personal info in same account
- 21% of mobile users share logins with families
- Mobile malware: apps
- Insufficient mobile platform security

Social Media Risks

- Consumer harm and reputational damage



K&L GATES

Example – “Peter Pan virus” phishing email (September 2014)

- Email purportedly came from real company BH Live
- Ticketing and entertainment company based in Bournemouth
- Claimed recipients had tickets to see Peter Pan
- Invited people to open attached e-tickets
- Opening attachment may have downloaded viruses
- BH Live inundated with phone calls from worried recipients

K&L GATES

Example 2 - G4S - fake website November 2014

- Cloned website set up at new virtually identical address
- Press release CFO sacked and accounts would need to be restated
- Caused share price to drop
- Estimated cost of registering fake website $20

Protection and Risk Mitigation

Why mitigate cyber risk?

Consequences of a cyber attack could be catastrophic

Consider

- How long could a business that relies on internet sales survive if no one could access its website?
- What would be the impact on its sales if no one was prepared to enter their credit card details?

Legal Consequences

- The Data Protection Act 1998 ("DPA") requires the data controller to implement appropriate technical and organisational security measures against unauthorised or unlawful processing, accidental loss, destruction or damage of personal data.

- Regulatory penalties may be imposed on the company for breach of the DPA including:
  - Fines;
  - Enforcement notices; and
  - Director disqualification

- Personal data owners may claim compensation from the data controller for such breaches under the DPA.

Practical Consequences

- As important to companies subject to a cyber attack are what the consequences of such an attack are in practice for the business.
- **Loss of customer information**, credit card details and other personal information.
  - Data owners seeks compensation against a business under the Data Protection Act, especially if the hacker cannot be identified.
- **Prevention of sales**.
  - Retailers with an online presence that are subject to a Denial of Service attack lose customers to competitors. You may eventually get your site back up, but will the customer be back?
  - This risk is heightened at times of traditional high online sales

Pro-active management at board level

- Not an IT problem - board level support is required to ensure that the resources both in time and capital are expended.
- *"Responsibility to manage your company's cyber risks starts and stops at Board Level. You can never be totally safe. Risks will, at times, become reality."* Sir Iain Lobban, Director, GCHQ 2012.
- Ensure that a cyber security management policy is part of the company's governance framework and that this is given the same level of attention as financial and other risk management regimes.

Pro-active management at board level (2)

How would the board answer the following questions:

- What strategy did you have in place to prevent this cyber attack from happening?
- Who was responsible for the strategy?
- What was done in advance to limit the damage from attacks of this nature?

Pro-active management at board level (3)

- Basic information risk management will highlight potential cyber attacks, allowing a board to see what constitute the most potent risks to the company.
- Understand
  - what data you hold
  - how sensitive the data is
  - which systems control the management of key information
  - how critical is the information to the management of the business

Ensuring internet safety and network security

- Methods to reduce cyber risk include:
  - **Mobile working** - ensure that a mobile working policy is in place to ensure the security of documents away from the office.
  - **Control access to removable media** such as memory sticks and removable hard drives and avoid their use where possible, especially with regards to storage of sensitive data. All removable data should be encrypted.
  - **Establish a policy on appropriate use** and educate staff regarding the appropriate way to use the company's IT systems.
  - **Implement an incident response plan** to ensure effective response to a cyber attack.

Ensuring internet safety and network security (2)

- **Create an incident management team** and provide specialist training to it who can carry out this process.
- **Control and limit access -** Only allow employees access to the information they require to carry out their roles.
- **Scan all media** before incorporating them into IT systems to detect any malware.
- **Monitor ICT systems** for unusual activity.
- **Implement malware protection** to all business areas and produce a policy on dealing with any malware issues.
- **Install security patches**
- **Implement basic security controls on networks**. Ex-employees should immediately be denied access.

Adequate training and internal procedures

- A cyber attack can take many forms including deliberate attacks, technology issues or simple human error or negligence.
- Every company has a cyber defence weak spot in its **own employees.**
- An adequate defence system protecting a company from cyber attacks should not only have the relevant defences and policies in place, but staff must be trained on the relevant policies.

Adequate training and internal procedures (2)

- Implementing staff training and clear mechanisms for staff to report concerns regarding other members of staff non-compliance with polices

- Not knowing what devices are held significantly increases a company's cyber risk profile

- Every company should draft and implement a home and mobile working policy, and train staff to adhere to it

Ongoing Management

- Planning and analysis of risk serves no purpose unless a company also properly implements its findings.
- As cybercrime evolves over time, companies must constantly monitor the adequacy of their cyber defences and re-evaluate the threats pertinent to their business.

Immediate damage to reputation

- Cyber attacks naturally affect customer confidence, especially when customer information or funds are stolen.
- Exacerbated by online communication forums that spread news of such an attack
- Crisis management costs include:
  - Informing affected customers;
  - PR campaigns to restore reputation;
  - Management time;
  - Retrieving data;
  - Suspending customer access to data and websites where relevant;
  - Forensic investigation of the attack; and
  - Repairing cyber defences.

Immediate damage to reputation (2)

- 82% of the UK public would stop dealing with an organisation if their online data was breached (Unisys survey, 2011)
- Brand damage may also come in the form of intellectual property infringement with fake websites or counterfeit products sold online.
- IP theft can result in loss of first-to-market advantage and a consequential loss of competitive advantage.

Possible long term impact on business strategy and financial stability

- Research and development may be scaled back to preserve current financial stability or because frequent IP theft has made it unprofitable.
- Businesses may shy away from exploiting the online market for fear of incurring another costly cyber attack

A growing issue

- Consumers are becoming increasingly receptive to interacting with businesses online
- As customer interaction with online technology grows, so too does their disclosure of sensitive, personal information.
- A cyber attack that results in a loss of customer information can cause huge reputational damage
- The prominence of social media and the speed at which information can be disseminated can cause reputational damage at an unprecedented speed.

Two further presentations

- Managing the Consequences of Data Breaches: US and Europe on 21 January 2015 will look at legislative changes that may lead to greater enforcement and substantial financial sanctions in the UK and internationally.
- Insuring against Cyber Risks on 25 February 2015 will look at the insurance market and consider the policies available and the areas where companies may wish to obtain legal advice.


K&L GATES