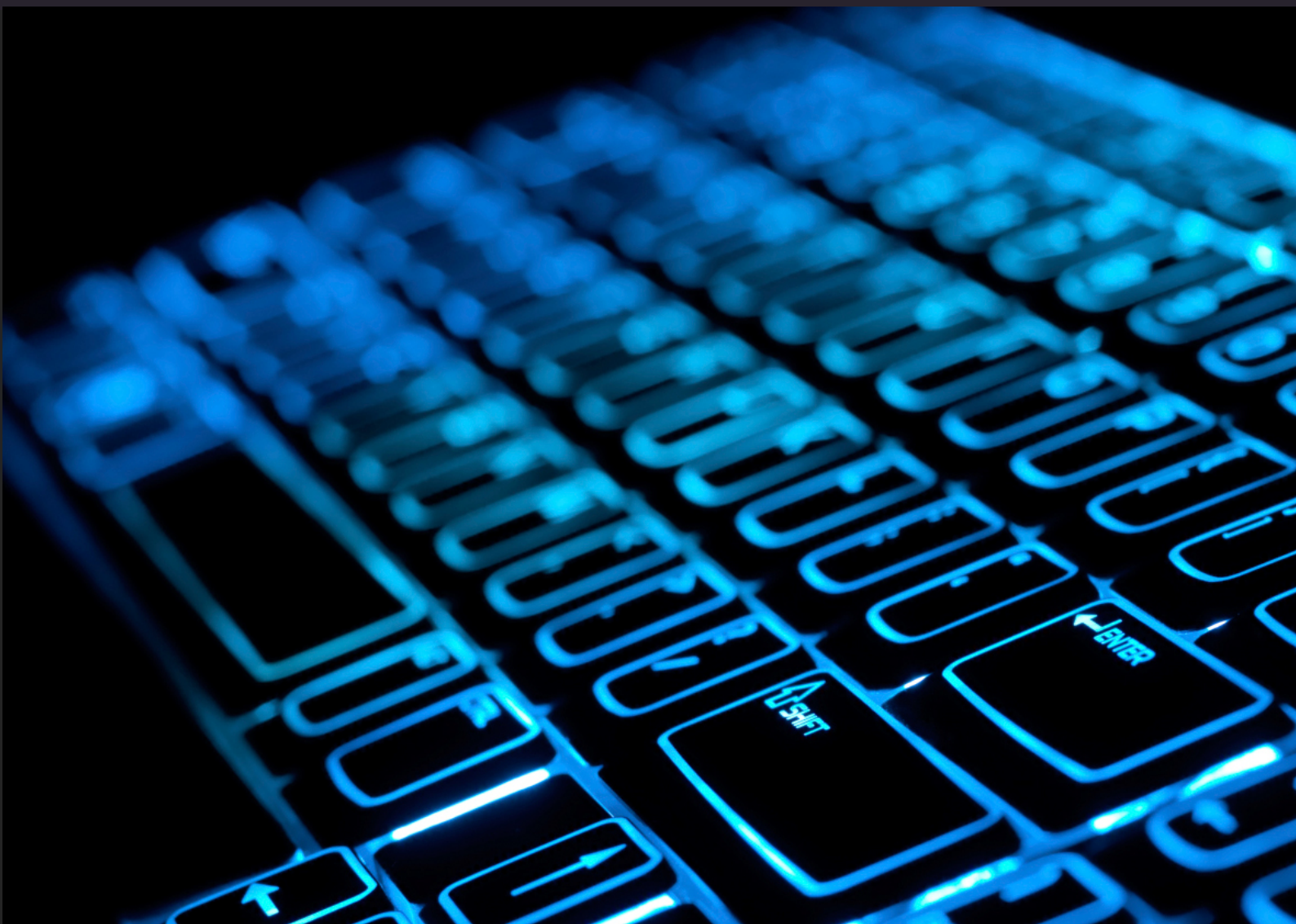
The Olswang Cyber Alert

October 2014

OLSWANG



Introduction and welcome

Welcome to the second 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. It is European Cyber Security month, and there is no doubt that cyber security is rising up the international as well as the business agenda. NATO recently adopted an amendment to its charter to put cyber attacks on the same footing as armed attacks – see paragraph 72 of NATO's **Declaration**,

In this edition:

- In our lead article, EJ Hilbert, Managing Director, Cyber investigations, Kroll EMEA, considers **the true cost of cybercrime;**
- In our **standards and benchmarks** section we consider the **new ISO standard** for processing PII in the cloud, new standardisation guidelines for **cloud computing SLAs** and look at the UK's new certification scheme **Cyber Essentials**.
- On our **regulatory radar** in this edition we track the progress of **EU legislation** on data and cyber breach notification, and draft **US legislation** and look in depth at new cyber security legislation in **France** and **Germany** and proposals to strengthen criminal penalties in the **UK**. We also look at a first of its kind **ruling** by the French data protection regulator, the CNIL, over **supply chain security breaches**, and at the impact **UK fines** are having on security compliance.
- In our **threat vectors** section we highlight just some of the breaches and threats which have been in the headlines over the summer.

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 email.

Ross McKean
Head of Data Protection
Olswang LLP

The True Cost of Cyber Crime

By E.J. Hilbert, Managing Director, Cyber Investigations, Kroll EMEA

One of the hottest debates in the information security world is estimating the true cost of cyber crime.

Several researchers have attempted to put a value on computer enabled/dependent crime: The 2013 McAfee report stated that cybercrime costs worldwide were £266 billion ($445 billion) annually. NetDiligence reported that the legal and operational costs associated with each stolen customer record in the US is $956, with the average US data breach /liability cost being $2.9 million. The Ponemon report placed the average cost incurred by a corporation for a data breach at $3.2 million.

The debate centers on the validity of the numbers with the question from those refuting them: if they are accurate, where are all the billionaire hackers?

Threats and Numbers

Before we address that question we must first understand why it is important to calculate the true cost of cybercrime.

There are various business and cultural reasons why it's important to quantify the effects of cybercrime, but a practical reason is penalizing the perpetrators. When I served as an FBI Special Agent, in order for a criminal to be prosecuted you had to prove that they had broken the law. Each law addressing cyber threats included a minimum required loss to the victim of $5000. In reality however, depending on the jurisdiction of the courts, many cases would not be prosecuted unless the loss was over $250,000. In addition, if the criminal was convicted of the crime, the prison sentence was also based on the total loss or cost associated with their criminal activity. Thus, loss/cost and how it is calculated is an integral part of prosecuting cyber criminals.

In order to address both sides of the debate over the true cost of cybercrime, we much first address the threats that make up the common definition of cybercrime.

Cybercrime can be broken down into four categories: Crime, Espionage, Warfare and Activism.

Calculating the cost for each of these is extremely difficult because the impact often cannot be measured in real time.

A cyber espionage attack where trade secrets are being stolen and used by a competitor may last several years without the victim being aware of the attack and therefore understanding and quantifying its impact.

A cyber warfare attack is intended to destroy systems and data so again, the true impact is unknown until the attack is completed.

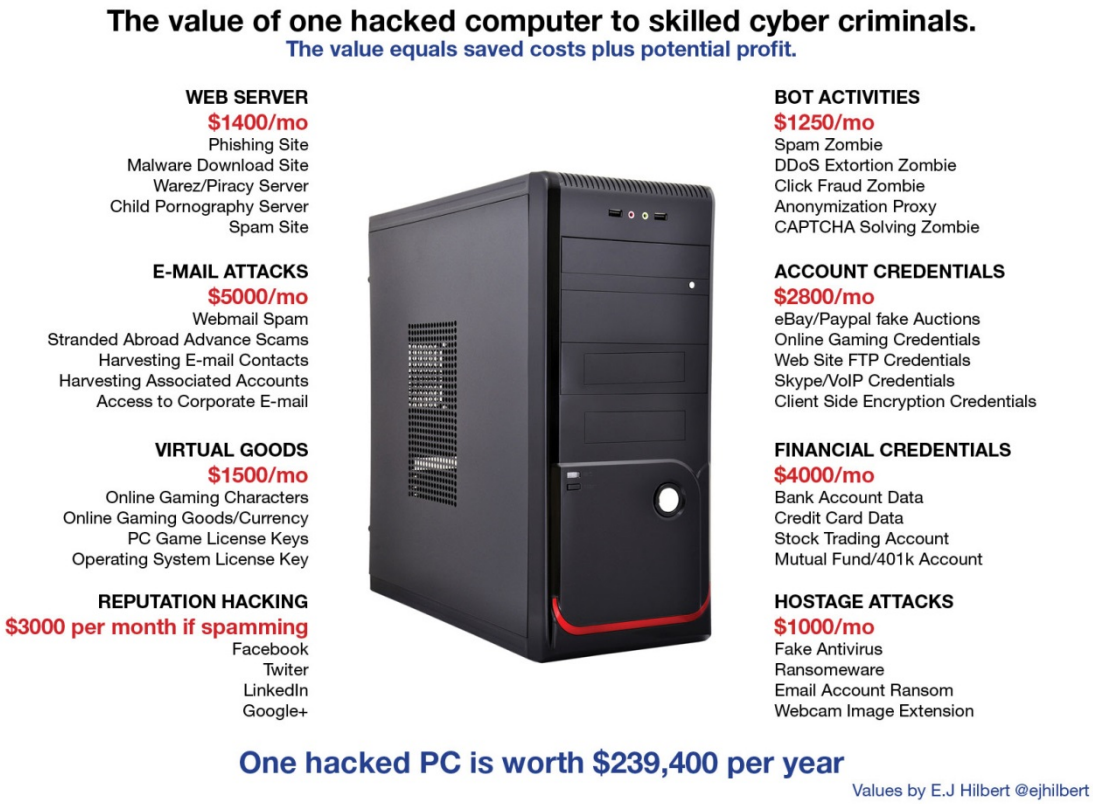
A cyber activist will attack a company and its management's reputation. It is an attempt to air a company's "dirty laundry" in order to force change within the company, but calculating the value of reputational damage is extremely difficult.

There are two sub categories of cybercrime: cyber-enabled crime such as hacking, malware delivery and botnet/DDOS attacks and cyber-dependent crime, which involves profit taking.

Cyber-dependent crime is where most media coverage is focused as it provides something tangible for people to understand. Namely, the data was stolen and used by criminals to buy products or steal money.

It is this belief of data monetization that fuels the debate about costs because we all assume that the fraud is the only cost. However, not all stolen data is credit/debit card numbers or financial information. Stolen data can be used in numerous different ways all of which result in profit to the criminals and costs to the victims.

Below is a graphic illustrating several ways a compromised computer can be used for profit.



The graphic shows eight potential uses for a hacked computer and within each of those eight, there are a minimum of four sub-uses.

The monthly values are based on a percentage of the reported losses from recent reports plus an average of the estimated cost for operation of systems from areas in the US, UK and other countries where the data could be obtained through public sources.

In order for a cyber-criminal to achieve $240K in a year, they must use the hacked box for all of the listed uses and sub-uses. They must also not be paying for the services such as the hardware itself, electricity,

installed software and internet bandwidth. The time expense of creating the email or social media accounts has also been excluded.

If a cyber-criminal is running any of these schemes, the “cost” is not only the profit being made but also the capital outlay the victim suffers to correct the issues.

The Costs

Based on the threats, cybercrime statistics must take into consideration all components of a cyber-related incident when calculating the “cost.” These components include:

- Man hours to fix the issue multiplied by the hourly rate of the employee
- Cost for consultants and outside experts
- Cost for new/updated equipment
- Cost of the reputational harm to the victim company
- Amount of fraud against stolen credentials
- Fraud dependent on stolen credentials
- Costs to replace stolen cards and data
- Costs for insurance
- Cost for data recovery
- Law suit liabilities
- Regulatory penalties

The inclusion of all of the above components into the cost calculation provides companies with a more complete picture of the true impact of an incident versus just the profit to the criminal.

Remediation

Firms often claim to understand cyber threats and will talk of technology and software defenses, new roles within management to ‘own’ cyber risk, but when asked about the efficiency and effectiveness of their cyber security efforts, they often struggle due to a lack of understanding. By understanding the costs and how they are calculated, companies can develop cost saving strategies in each area.

For example, conducting a proactive/pre-incident system assessment will reveal potential gaps in the security posture to be addressed. Equally, a review of policies and procedures by external specialists who understand the company’s systems prior to an event will dramatically cut costs because plans for incident management and resilience will already exist. The same can be said for relationships with law firms, insurance companies and public relations companies which can provide:

- Proactive risk assessments
- Legal advice
- Crisis management and remediation planning
- Communications plans to avoid reputational damage
- Insurance cover for losses

It should also be noted that the draft EU General Data Protection Regulation includes new mandates on how data is handled, how breaches are reported and penalties equal to 5% of a company's gross annual turnover. Companies that do not understand the threats, costs and impact in advance of an incident are going to suffer the most. Preparation based on understanding is the key.

Final thoughts

The true cost of cybercrime is not just the monies made by the criminals or the cost of legal liability; it is the combination of all systems and people impacted. Cyber-attacks are no longer a matter of "if" but a matter of "when." As such, understanding the threat, the uses of the data, the impact of the incident and the breakdown of the costs is pivotal to the defence and resilience of a company.

EJ Hilbert, Managing Director, Cyber Investigations, Kroll EMEA

Standards and benchmarks

Cyber security standards and benchmarks

New ISO 27018 Code of practice for protection of PII in public clouds

In August this year the ISO published a new security standard for cloud services: ISO/IEC 27018 – *Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors* ("**ISO 27018**"). Datonomy reported in May this year that this new standard was on its way. This publication is a welcome step towards ensuring compliance with the principles of privacy laws and further boosting customer confidence in cloud computing technologies. Read our full summary here.

EU: New standardisation guidelines for cloud computing services SLAs

As reported on Datonomy here, these new guidelines were published in June by the Cloud Select Industry Group.

Forming part of the European Commission's wider Cloud Computing strategy which was unveiled in 2012, the guidelines have been described as a first step towards standardised building blocks for terminology and metrics in cloud SLAs. They aim to improve the drafting clarity and customer understanding of cloud SLAs. European Commission Vice-President Viviane Reding said: "*[the] new guidelines will help generate trust in innovative computing solutions and help EU citizens save money. More trust means more revenue for companies in Europe's digital single market."* The 62 page guidelines – created by a drafting team which included participants from IBM, Amazon, Microsoft and T-Systems – deal with service levels relating to availability, reliability, security, support services and data management, and take into account the guidance of the Article 29 Working Party.

UK: Cyber security certification scheme launched

As reported on Datonomy here, following the consultations on the requirements for a preferred standard for cyber security, which concluded in November 2013 (background information here), the Government has launched a new cyber security certification scheme. The scheme focuses on five main controls for basic cyber hygiene:

- boundary firewalls and internet gateways;
- secure configuration;
- access control;
- malware protection; and
- patch management.

Businesses can apply for a “Cyber Essentials” certificate (based on independently verified self-assessment) or a “Cyber Essential Plus” certificate (offering a higher level of assurance through external testing). The scheme is designed to be affordable and offers a snapshot of the organisation’s cyber security effectiveness on the day of assessment. Guidance on meeting the Cyber Essentials requirements can be downloaded from the government-approved cyberstreetwise website here, and a summary of the scheme can be found here. Vodafone has become the first telecoms company to gain the UK ‘cyber essentials plus’ accreditation.

UK: impact of ICO fines on data security

As reported on Datonomy here, the ICO has published a review of the impact of its civil monetary penalties (“CMPs”), the vast majority of which have related to security breaches. The review canvassed the views of representatives from 14 organisations who had received a CMP and 85 peer organisations who had not. The findings suggest that overall CMPs are effective at improving data protection compliance. However some respondents felt that there was a lack of transparency about how CMPs have been calculated and some showed a lack of understanding of just what poor practices trigger the CMP threshold.

Regulatory radar

NATO

There is no doubt that cyber security is rising up the international agenda, with the recent adoption by NATO of an amendment to its charter to put cyber attacks on the same footing as armed attacks. This recognises that a cyber attack's *"impact could be as harmful to modern societies as a conventional attack"* (as stated in NATO's Declaration, at paragraph 72). In its declaration, the alliance also said that it will further develop national cyber defence capabilities, including endorsing better information sharing, to make the organisation better protected.

EU: progress on draft NISD and GDPR

The summer has seen much institutional change in the EU, first with the European Parliament elections in May, the start of Italy's Council Presidency in July and now with the reorganisation of the European Commission and appointment of a new Commission President and Commissioners with effect from 1 November. As reported in our first edition, there are two proposals making their way through the Brussels legislature which will change the legal landscape for the reporting of cyber attacks. These are the draft **Network and Information Security Directive**, which will impose reporting obligations on providers of critical infrastructure, and the draft **General Data Protection Regulation** which will impose data breach reporting requirements on all data controllers. The summer has seen little procedural progress, although trilogue negotiations on the NISD have now begun, and on the GDPR the Council (representing the Member States) has, according to this Council press release, just reached a broad consensus on the security and breach provisions in Chapter IV of the GDPR – although the Council has not yet agreed its position on the whole proposal. We summarise the current state of play on both proposals here.

France

Meanwhile, certain Member States are pre-empting the adoption of the NISD with their own cyber breach legislation. We take an in-depth look at France's Military Programming Act. A first-of-its-kind regulatory action against Orange by the French data protection regulator, the CNIL, over a data security breach in its supply chain, is reported here.

Germany

Germany has also proposed its own regime – we look at the latest proposals for an IT Security Act here.

UK

The UK's proposals for tougher sentences for serious cyber attacks under the Computer Misuse Act 1990 are reported here.

US: We report on proposals for the controversial Cybersecurity Information Sharing Act here.

Threat vectors

A small selection of the cyber threats and statistics that have made recent headlines.

- Sources including censorship watch dog *GreatFire* have alleged that the Chinese authorities are staging a "man-in-the-middle" attack on Apple's iCloud, just days after the iPhone went on sale in China. The attack is designed to intercept user's iCloud account usernames and passwords, using a fake login site that looks exactly like the Apple iCloud login site. Read more from *The WHIR* and *ITProPortal.*
- A new bug, which could be affecting hundreds of millions of computers, servers and devices using Linux and Apple's Mac operating system, has been discovered. System administrators have been urged to apply patches to combat the bug, which has been dubbed "Shellshock". Read more from the *BBC.*
- US companies Home Depot, Supervalu and JPMorgan Chase & Co have all been hit by high profile cyber attacks.
- Mark Boleat, head of policy for the City of London, has echoed comments made by New York's financial regulator Benjamin Lawsky that an "*Armageddon style*" cyber attack will trigger the next global financial crisis by making a major bank "*disappear*". Mr Boleat also said that the City of London police had uncovered a *"huge underground economy, and a huge underground network"* capable of conducting movie-style cyber attacks. Read more from *The Telegraph*.
- As has been widely reported, there has been an extremely targeted hack against celebrities, resulting in numerous nude photographs being temporarily floated in the public domain. In the fallout, cyber-thieves reportedly sent out fake notification messages to iCloud users to trick people into handing over their login details.
- Similarly, 13 GB worth of photos from popular mobile phone app Snapchat have been dumped online. The attack has been dubbed "The Snappening" and was carried out by the use of insecure third-party software designed to let users store "disappearing" snaps. Many are blaming Snapchat for the breach. Read more from *The Independent.*
- Security firm Hold Security has announced the "*largest data breach known to date*", after a Russian gang dubbed "CyberVor" stole over 2 billion credentials. More details here and here.
- As *ZDNet* reports, new research published by FireEye claims that 68% of the most popular free Android apps could become a pathway for cybercriminals to lift sensitive data.
- An interesting blog by *CBR* highlights six cyber security trends to watch out for during the rest of 2014, which includes more focus being placed on cyber education and an increase in infrastructure targeting by hackers.
- The *"very alarming"* level of cyber threats organisations face is unlikely to fall for at least 10 years, says Suleyman Anil, head of cyber defence at the emerging security challenges division of NATO. Mr Anil asserted there are three prime reasons for this; cyber crime is low risk with the promise of high profits, there has been an increase in opportunity to attack systems and most worryingly, there is growth in state-sponsored cyber attacks. Read more here.

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

Christian Leuthner
Associate, Munich
+49 89 206 028 414
Christian.leuthner@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 89 206 028 404
andreas.splittgerber@olswang.com

Elle Todd
Partner, London
+ (0)20 7067 3105
elle.todd@olswang.com

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

Claire Walker
PSL, London
+44 (0)20 7067 3174
claire.walker@olswang.com

Katharine Alexander
Trainee Solicitor, London
+44 (0)20 7067 3560
katharine.alexander@olswang.com

Tom Errington
Paralegal, London
+44 (0)20 7067 3813
tom.errington@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

17999796-1