



Cambridge Centre for Risk Studies
Advisory Board Research Showcase – 23 January 2018

Cyber Risk Insight

Centre for
Risk Studies



UNIVERSITY OF
CAMBRIDGE
Judge Business School

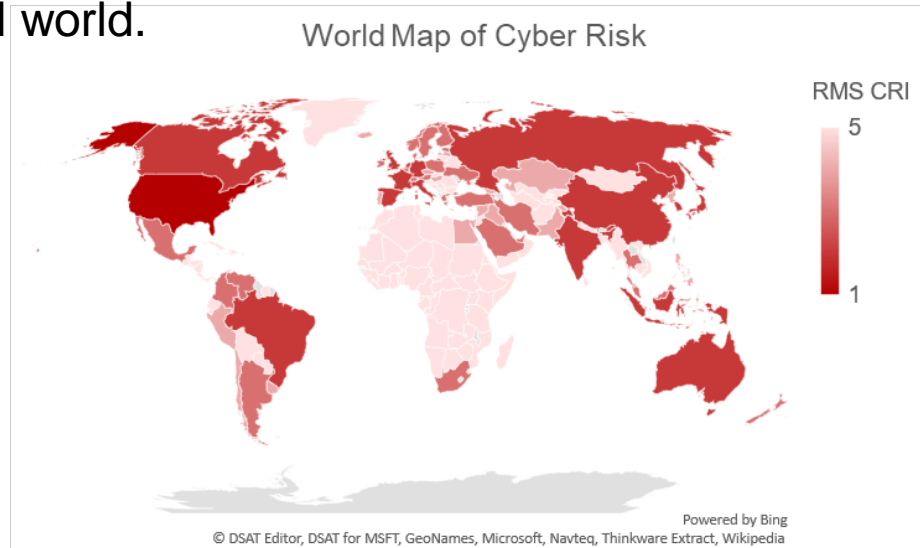
Dr Jennifer Daffron
Research Associate
Cambridge Centre for Risk Studies

Themes of the Cyber Risk Landscape

- The Internationalisation of Cyber Threat
- Exfiltration Events Morphing into Extortion
- The Importance of Patching Cadence
- Rise of Cryptocurrencies
- Changes in Data Regulation: GDPR

The Internationalisation of Cyber Threat

- Cyber losses are now being reported in almost every country of the industrialized world.



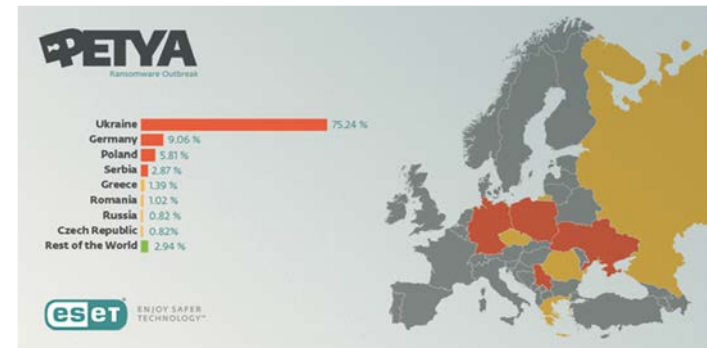
- Individual malware attacks flow across international borders

WannaCry - May 2017
150 countries

The 'Wannacry' ransomware attack
The attack has hit more than 200,000 victims in at least 150 countries, says Europol



NotPetya - June 2017
65 countries



Exfiltration Morphing into Extortion

- External attacks to steal personal data are not as profitable as they have been in the past
 - Black market prices have reduced per record
 - Many of the dark web sites have been closed down
- Extortion payments now a more common mode of exploiting cyber attacks across several loss processes (DDoS, Malware, Data Exfiltration)
- We are seeing more cases of large companies paying substantial ransom fees to redeem their data
 - Web hosting company Nayana, South Korea
 - Erebus ransomware on June 10
 - Paid out 397.6 Bitcoin - approximately \$1 million



WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017

ADVERTORIAL

BUCKLE UP FOR A BUMPY 2018
AS CYBER-EXTORTION HITS
NEW HIGHS

What a 12 months we've had. The threat landscape has evolved again and again during 2017 to net cybercriminals billions and cause chaos, destruction and political turmoil in the process



Ooops, your files have been encrypted!

English



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Mondays to Friday

Payment will be raised on

5/15/2017 20:34:43

Time Left

02:23:53:13

Your files will be lost on

5/19/2017 20:34:43

Time Left

06:23:53:13

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

115p7UMMngo1pMvkcHijcRdfJNXj6LrLn

Copy

Check Payment

Decrypt

The Importance of Patching Cadence

■ Equifax

- Security vulnerability CVE-2017-5638 public in March 2017, but Equifax failed to fix the bug in their networks
- Sensitive personal records, including social security numbers, of more than 140 million folks in the US, UK and Canada.
- 143 Million people effected.

■ WannaCry Attack

- UK NHS, FedEx Corp, Telefonica, Renault, Russian Railways...
- In March, Microsoft discovered a vulnerability and issued a patch but not everyone updated their systems.
- Then in April, information was stolen (or leaked, no one is sure at this point) from the NSA that revealed the specific vulnerability and a hacking group sold the information.
- 200,000+ computers across 150 countries.

■ 'Chipmageddon'

- Meltdown & Spectre Exploits: allow an adversary to access kernel-level memory without proper security checks, potentially gaining access to passwords and other sensitive information cached in memory.
- The Register broke the story on 2 January 2018 before Intel and other technology and software companies were able to release the necessary patches
- 3 billion computers, smartphones, tablets and other devices are vulnerable to Spectre.

Cryptocurrencies

- Cryptocurrency and the development of ransomware has established an easier method for threat actors to profit from cybercrime
 - Bitcoin, Ripple, Ethereum
 - Digital currencies encourage victim payment through malware and ransomware to almost untraceable cybercriminals.
 - Preferred payment method between criminals to purchase illegal goods and services online.



- **Bitcoin's** booming value has driven a huge rise in crypto-currency themed malware, say security firms.

- WannaCry
- NotPetya
- Bad Rabbit



The General Data Protection Regulation (GDPR)

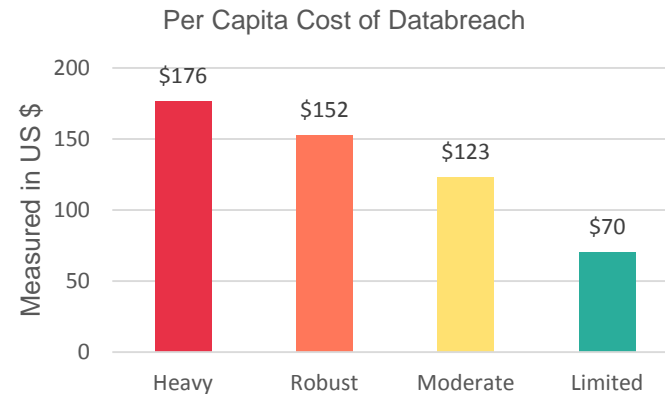
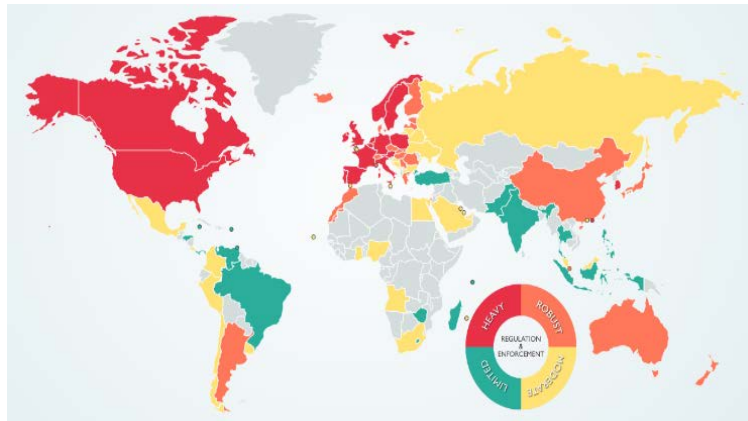
- On 25 May 2018 GDPR aims to combat the growing trends in data exfiltration by standardising data protection laws.
- What information does GDPR apply to?
 - **Personal data:** any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, **online identifier** or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.
- GDPR Jurisdiction
 - Those companies currently subject to the UK Data Protection Act 1998
 - Any company offering goods or services (even for free) to EU citizens or any monitoring of EU citizens
- Noteworthy Changes:
 - The Accountability Principle
 - Breach Notification
 - Restrictions on the Transfer of Data
 - Increased Fines



The General Data Protection Act

■ Increasing the cost of a data breach?

Those countries with the strictest regulations on data breach yield the highest cost per capita of data breach, with companies in heavily regulated countries paying over twice as much per record than those countries with limited data regulation.



Not a matter of *if*, but *when*...

CASSANDRA.com Sign up Log in

Hypothetical News TV & Video International Business Sport Entertainment

Contagious Malware Costs \$10 Billion

The economic cost of the latest Malware hits all-time high

Friday, November 9

New York, NY (2251 GMT – 1751 EST) - The \$25,000 decryption key for the newest strain of ransomware has millions of individuals across the globe desperate for a solution.



CASSANDRA.com Sign up Log in

Hypothetical News TV & Video International Business Sport Entertainment

BREAKING NEWS

Spyderbyte Transmission Site

Contagious Malware traced to North Korea, investigation finds

Monday, September 23

Beijing, China (0246 GMT – 0946 CST) - Seventy-two hours after the first reported case of 'Spyderbyte', US officials have identified a North Korean state-sponsored hacking group responsible.



CASSANDRA.com Sign up Log in


Hypothetical News TV & Video International Business Sport Entertainment

Chipmageddon Crisis Point

Meltdown & Spectre to blame for largest recorded data breach

Thursday, September 12

Singapore (0343 GMT – 1143 SGT) - As the patches are slow to roll out, hackers continue use these vulnerabilities to steal sensitive information.



Meltdown and Spectre affect numerous Intel, AMD and ARM chips on laptops, desktops, servers, tablets and smartphones. All operating systems (Apple products are affected too), internet browsers and several other commonly used applications are also releasing updates to address

These exploits have highlighted a serious security flaw that have some in the IT community wondering if a hardware redesign is necessary for future CPUs and leaving businesses with increased processing time for

CASSANDRA.com Sign up Log in

Hypothetical News TV & Video International Business Sport Entertainment

Ecommerce takes another hit

DDoS attacks wreak havoc on ecommerce market

Monday, May 12

Sydney (2308 GMT – 0808 Aus EST) - Companies in the ecommerce sector continue to be the favoured target for DDoS attacks.



Centre for **Risk Studies**



UNIVERSITY OF
CAMBRIDGE
Judge Business School

Dr Jennifer Daffron
j.daffron@jbs.cam.ac.uk
+44 (0) 1223 761075