Institute
and Faculty
of Actuaries

Cyber Risk Symposium

What do good cyber practices look like and, to what extent, can we as an industry implement these operationally

10 February 2020

Agenda

17:30 – 17:35	Chairman’s introduction
17:35 – 17:45	How you can all benefit from the work of the Cyber Risk Investigation Working Party
17:45 – 17:55	Do past incidents predict those in the future?:
17:55 – 18:05	A CISO's perspective on managing Cyber Risk
18.05 – 18:15	Quantifying cyber risk – an introduction to an academic paper on modelling Cyber Risk
18:15 – 18:25	Challenges with quantifying cyber risk from an academic perspective
18:25 – 18:50	Good practices for bad times
18:50 – 19:15	Panel discussion: Is good achievable? How can we work better together to achieve a better outcome and how do you measure what good looks like?
19.15 – 19:20	Closing remarks
19:20 – 20:30	*Drinks and Networking*

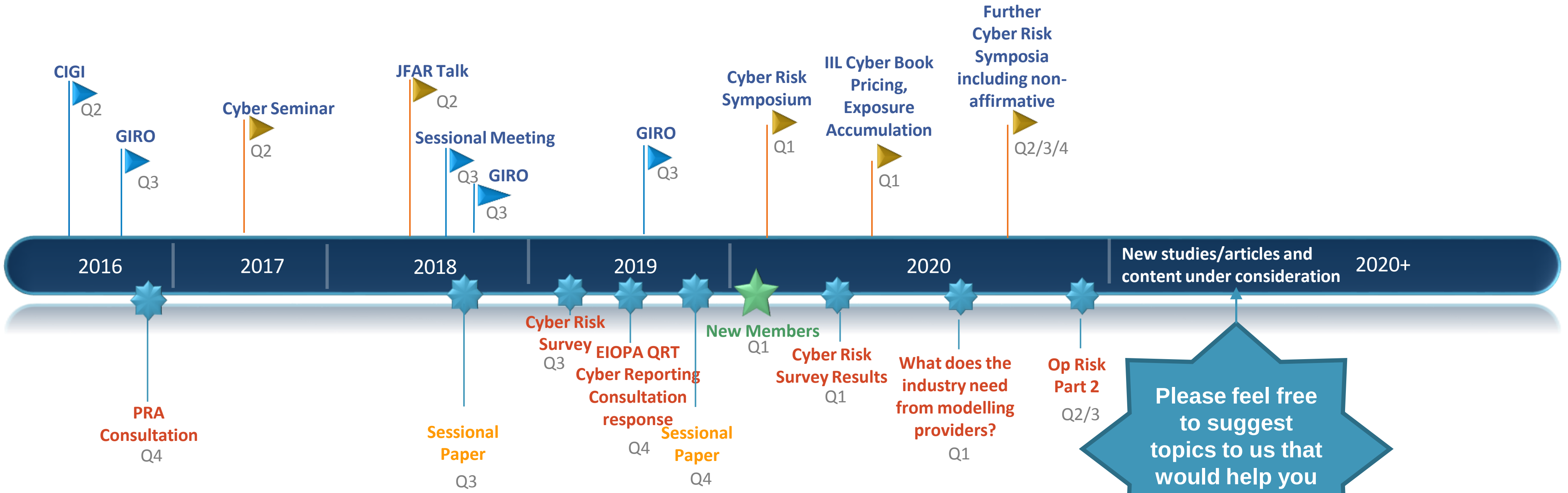
Institute
and Faculty
of Actuaries

How you can all benefit from the work of the Cyber Risk Investigation Working Party

Visesh Gosrani

10 February 2020

How you can make use of our work to date and to come



CIGI Q2

GIRO Q3

Cyber Seminar Q2

JFAR Talk Q2

Sessional Meeting Q3

GIRO Q3

GIRO Q3

Cyber Risk Symposium Q1

IIL Cyber Book Pricing, Exposure Accumulation Q1

Further Cyber Risk Symposia including non-affirmative Q2/3/4

2016

2017

2018

2019

2020

New studies/articles and content under consideration

2020+

PRA Consultation Q4

Sessional Paper Q3

Cyber Risk Survey Q3

EIOPA QRT Cyber Reporting Consultation response Q4

Sessional Paper Q4

New Members Q1

Cyber Risk Survey Results Q1

What does the industry need from modelling providers? Q1

Op Risk Part 2 Q2/3

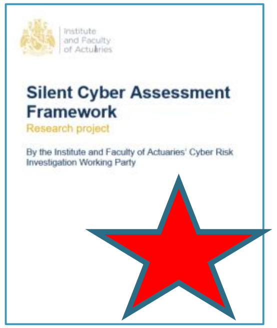
Please feel free to suggest topics to us that would help you in your roles

Institute and Faculty of Actuaries

Cyber operational risk scenarios for insurance companies

Research project

By the Institute and Faculty of Actuaries' Cyber Risk Investigation Working Party



Institute and Faculty of Actuaries

Silent Cyber Assessment Framework

Research project

By the Institute and Faculty of Actuaries' Cyber Risk Investigation Working Party

Output of the working party at
https://www.actuaries.org.uk/practice-areas/risk-management/risk-management-research-working-parties/cyber-risk-investigation

Join the community on LinkedIn
Group: "Cyber Risk + Actuaries"

Institute and Faculty of Actuaries

SCOR
The Art & Science of Risk

Do Past Cyber Incidents Predict the Future?

Richard Campanha
rcampanha@scor.com

10 February 2020

Antitrust Statement

A meeting such as this, including companies that compete, can serve many useful and pro-competitive purposes.

At the same time, these meetings have the potential to be misinterpreted and bear the risk to be misused to exchange competitive information that may limit competition.

To minimize this risk, I hereby remind you that during this presentation I will discuss matters of common interest regarding industry sound practices and the companies' and industry's relationships with the various governmental entities under which member companies operate.

This meeting will not be used to discuss (or agree on) pricing or any other competitive information; will not be used to discuss how any of our member companies compete in the market; and will not be used to discuss any joint action in any marketplace."

Disclosure

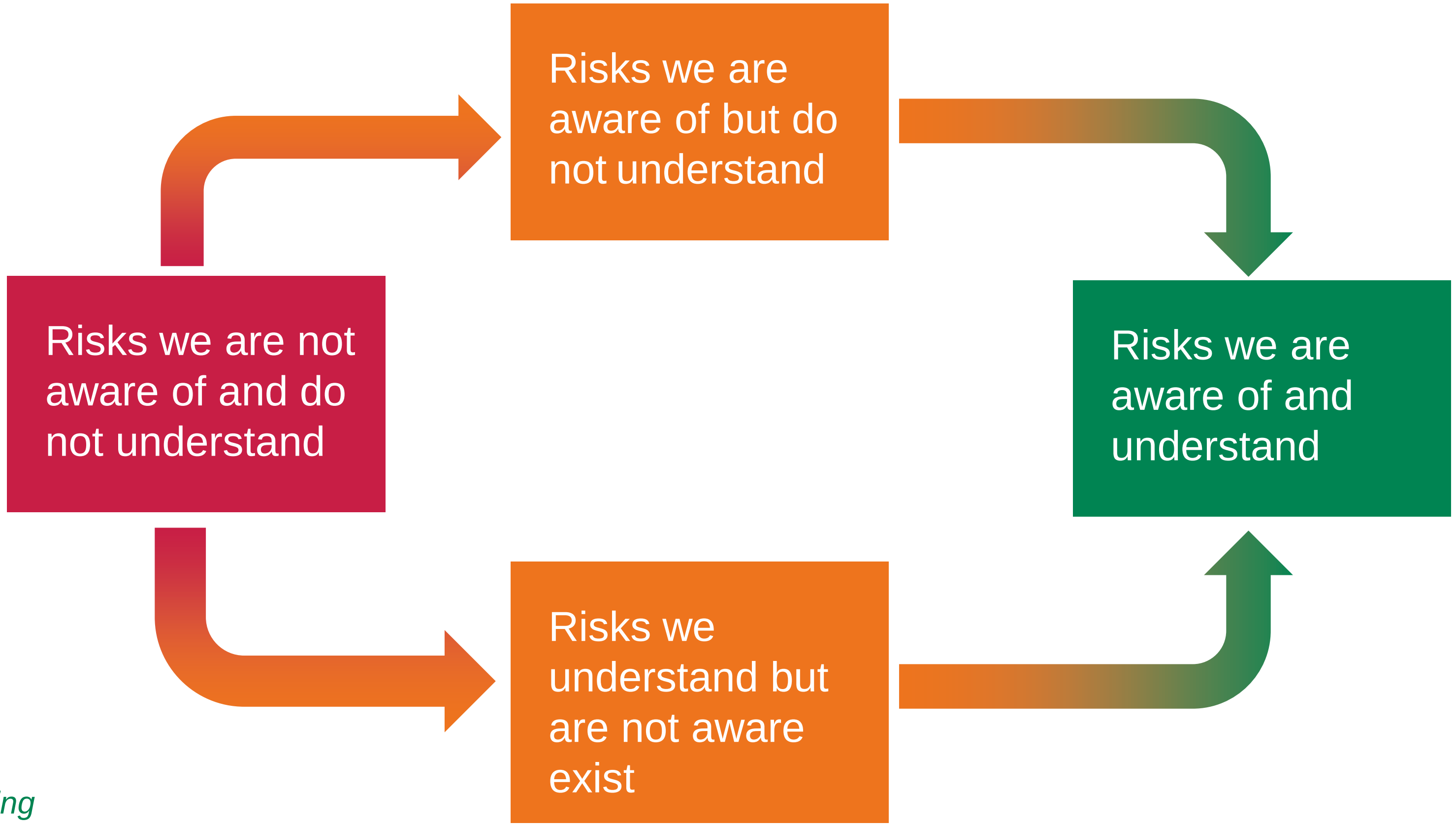
I am not affiliated with any of the companies referred to within this presentation nor any of their products.

Executive summary

- Historical Events
- Human Error vs. Malice
- Frequency and Severity of Future Incidents
- Future Incidents – A Prediction for 2020 (using this approach)

Historical Events

Flow of Data Gathering - What events can and cannot be modelled?



Risks we are not aware of and do not understand

Risks we are aware of but do not understand

Risks we understand but are not aware exist

Risks we are aware of and understand

Color Chart

- *Data exists to support modelling*
- *Field data may be gathered for future modelling*
- *Data doesn’t exist to support modelling*

Time axis

Historical Events

What events can and cannot be modelled?

What can be modelled?

- **Aware of and Understood**
    - Previously discovered and patched exploits
    - E.g. Code Red (2001), Conficker (2008), Not Petya (2017), WannaCry (2017), CVE-2020-0601 (Jan 2020)
- **Aware of but not Understood**
    - An attack that is discovered, but at the time unknown as to how it functions
    - E.g. Stuxnet (2010), Shamoon** (2012)
    - The Iranian attack on The Sands Hotel Las Vegas, NV (2014)
        - HR job listings can expose infrastructure
- **Unaware of but Understood**
    - Advanced persistent threat actors
    - E.g. an attacker gathering data for years for insider trader on a potential M&A

What can't be modelled?

- Unaware & Not Understood
    - Attacks that go undiscovered, unnoticed, and unreported by security specialists
    - E.g. Rate of occurrence of undiscovered Zero-day exploits

	Understood	Not Understood*
Aware	Risks we are aware of and understand	Risks we are aware of but do not understand
Unaware	Risks we understand but are not aware exist	Risks we are not aware of and do not understand

Color Chart

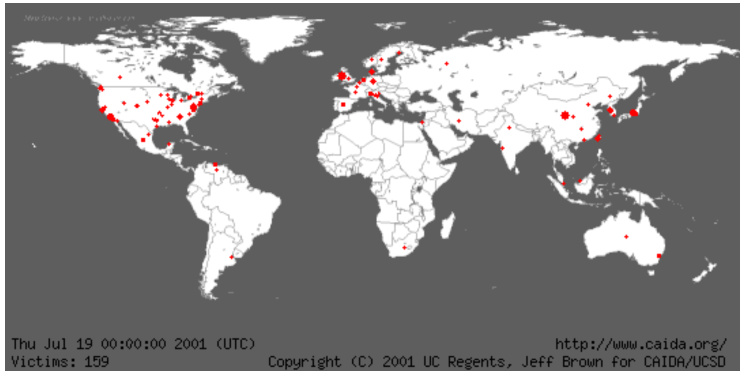
- *Data exists to support modelling*
    - *Fewer Modelling assumptions*
- *Field data may be gathered for future modelling*
    - *Many modelling assumptions needed*
- *Data doesn't exist to support modelling*

- *Donald Rumsfeld's "Known Unknown" chart rephrased.
- ** Attacked Saudi Aramco – causing 30k computers to go down. This later impacted the price of hard drives.

Historical Events

Can Cyber be Modelled *like* Pandemic Diseases?

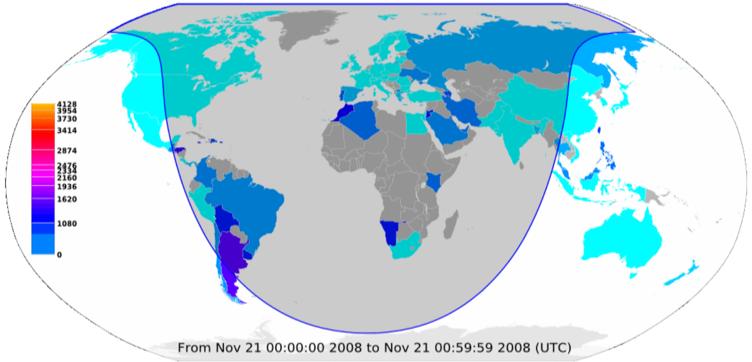
Code Red


Thu Jul 19 00:00:00 2001 (UTC)
Victims: 159
http://www.caida.org/
Copyright (C) 2001 UC Regents, Jeff Brown for CAIDA/UCSD

Zika Virus

ZIKA OUTBREAK
2013
2014
2015
2016
2017
2018

Conficker



WannaCry & NotPetya

- Code Red Source: CAIDA & http://thecyberrecce.net/category/worms/
- Zika Source: https://giphy.com/gifs/discoverychannel-discovery-mosquito-vzV2w9261pj4Q
- Ransomware Source: https://news.thewindowsclub.com/ransomware-attacks-reach-new-levels-sophistication-90521/
- Conficker Source: https://www.caida.org/research/security/ms08-067/telescope.tcp445.nov21.norm.log.animated.gif

Historical Events

Patching Releases Increase Infection Rate

- MS08-067 Patch – Zero Day (hard to predict)
  - Patched a proto Conficker worm
  - Outbreak analogous to Pandemics:
    - Small number of instances spread across individual networks

- Conficker Worm
  - MS08-076 Critical patch announcement (NSA involvement) led to the patch being reverse engineered into new attacks by copycat attackers. Increasing the frequency of attacks on unpatched systems.
  - Self replication analogous to a virus
  - Public ports, specially crafted message (RPC)
  - No downloads needed to be infected
  - In hindsight copycats are predictable
  - Led to a race to infect unpatched computers
  - Contact via active RPC port resulted in infection
  - Resultant: Remote Control Execution (RCE)

- To this day an estimated 400k computers are still believed to be infected by Conficker

- MS17-010
  - Eternal Blue (NSA again) leak led to patch announcement
  - Variants of Eternal Blue from patch (WannaCry, NotPetya)
  - Attacked via exposed SMB ports
  - NotPetya may be classed as ***cyber warfare*** rather than RansomWare (Mimikatz + Eternal Blue)

Dark Net Diaries Ep 57: MS08-067

- https://darknetdiaries.com/episode/57/
- *https://docs.microsoft.com/en-us/archive/blogs/johnla/the-inside-story-behind-ms08-067
- RPC = Remote Procedure Call, SMB = Server Message Block

Human Error vs. Malice

Verizon 2019 Data Breach Investigation Findings

- “System Admin related breaches on the rise. due to misconfigured servers”
- Organized Crime, “Hacktivists”, Espionage would fall under malice
- Notably, Organized Crime seems to be negatively correlated to State-Sponsored attacks (DarkMatter/Project Raven style correlation?)

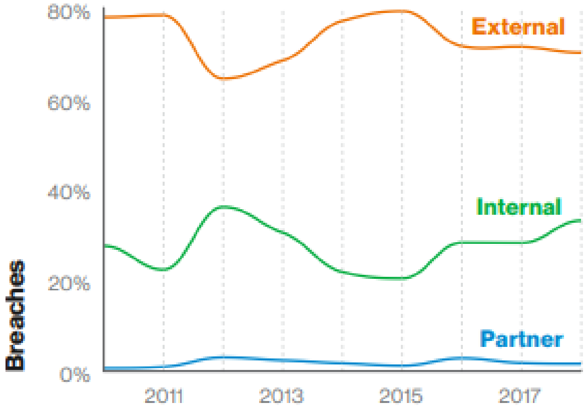


Figure 6. Threat actors in breaches over time

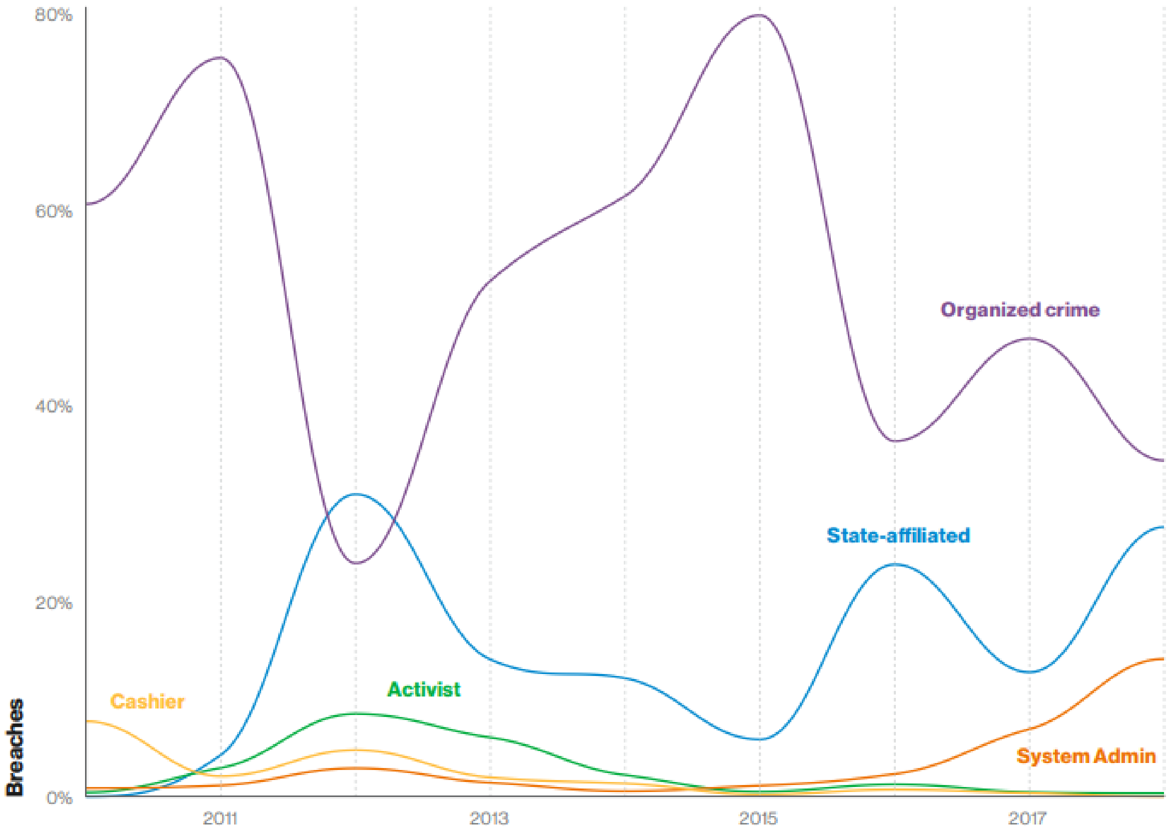


Figure 8. Select threat actors in breaches over time

1. Figures 6 & 8 taken from Verizon 2019 Data Breach Investigations Report.
https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
2) 50k botnets removed from figure 6 (attributed to External category).
3) Cashier includes bank tellers, point-of-sale terminals.

Frequency & Severity of Future Events

Economic Measures for Incentives of RansomWare

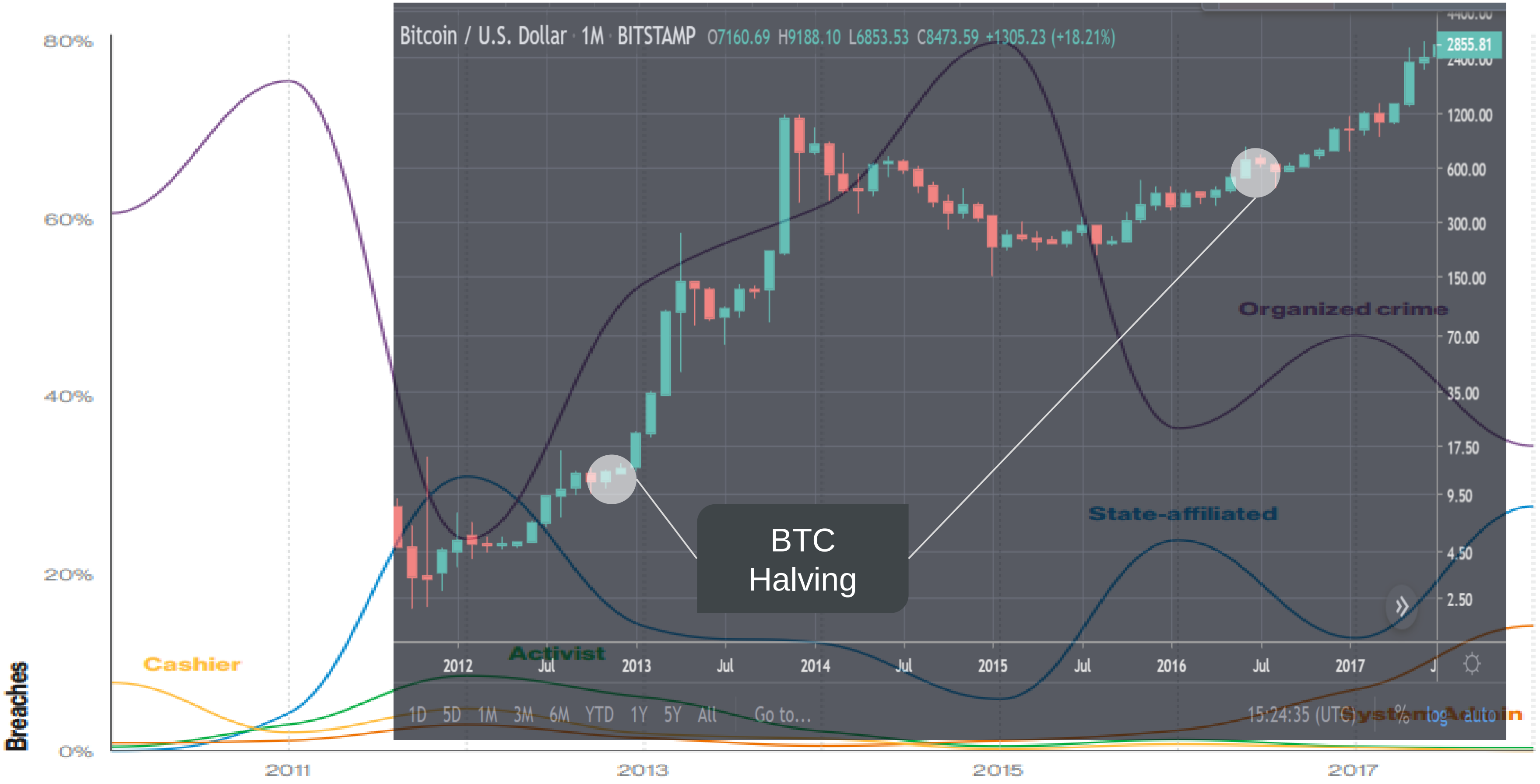


Figure 8. Select threat actors in breaches over time

- Lagging correlation between Organized Crime events BTC
- Creating and releasing malware takes time
- This can cause crime to lag behind BTC when BTC gaps as it did in November 2013.

Note BTC:USD is in log scale. Halving dates in footnote.

- Breach graph taken from Verizon 2019 Data Breach Investigations Report.
- 50k botnets removed from figure 6 (attributed to External category).
- Bitcoin Chart taken from TradingView.com using BITSTAMP exchange data.

- First BTC Halving Nov 2012
- Second BTC Halving Jul 2016
- Third BTC Halving May 2020

Frequency & Severity of Future Events

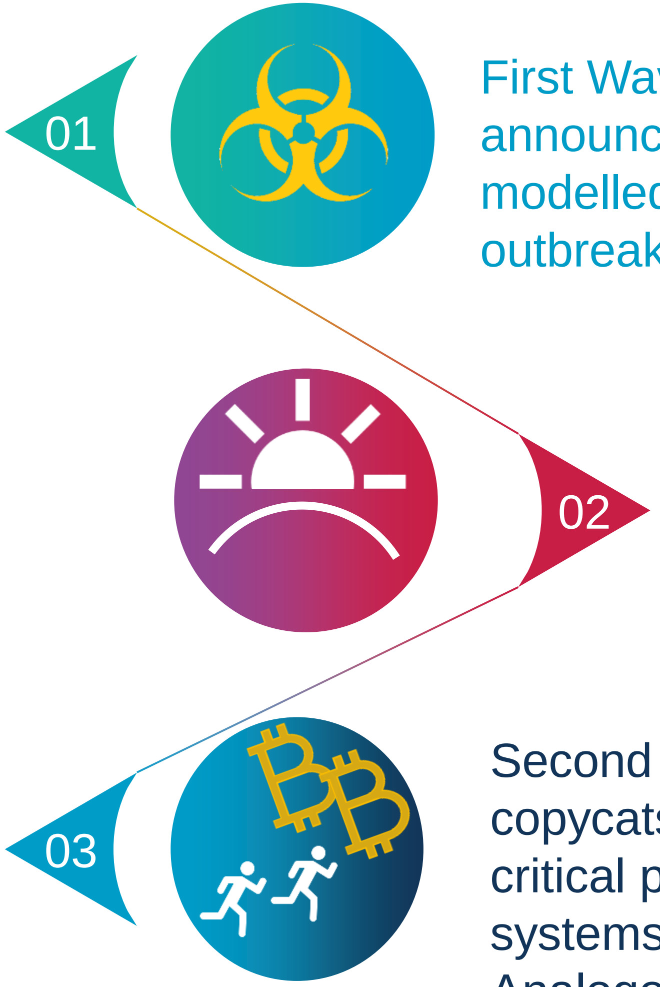
Modelling Frequency & Severity

- CVSS (Common Vulnerability Scoring System) score may be a good way to measure the susceptibility of a reverse engineered patch and to fine tune thresholds between first and second-wave stages.

- As a Patch is announced frequency of future (second-wave) infections may be potentially modelled by:
  - $f \propto 1 - \frac{dp_a}{dt}$
  - Where p_a is patch adoption as a percentage
  - Severity would be bespoke to each target and harder to estimate.

- As a measure of RansomWare severity of second-wave attacks may be potentially modelled via Bitcoin valuation:
  - $s \propto \frac{dB}{dt}$
  - Where B is the spot price of BTC:USD

- Alternative approaches for the second-wave attack stage:
  - Hunter-Prey model
  - Lanchester Combat model
  - Markov Chain, Monte Carlo, Logistic map models



First Wave attacks: Prior to a critical patch announcement cyber attacks may be modelled as the beginning of a **pandemic** outbreak

A critical patch announcement may be treated as a **threshold** where the pandemic model *transitions* to a race or hunter prey model

Second wave attacks: Cyber criminal copycats **rush** to reverse engineer the critical patch and infect unpatched systems with RansomWare Analogous to Viral mutation

- Note: State sponsored attacks may tend to target national holidays. The day these attacks strike may already be known, but not the year. This may not be true for countries used a testing grounds or those affected as collateral damage.

Future Incidents

A Prediction for 2020

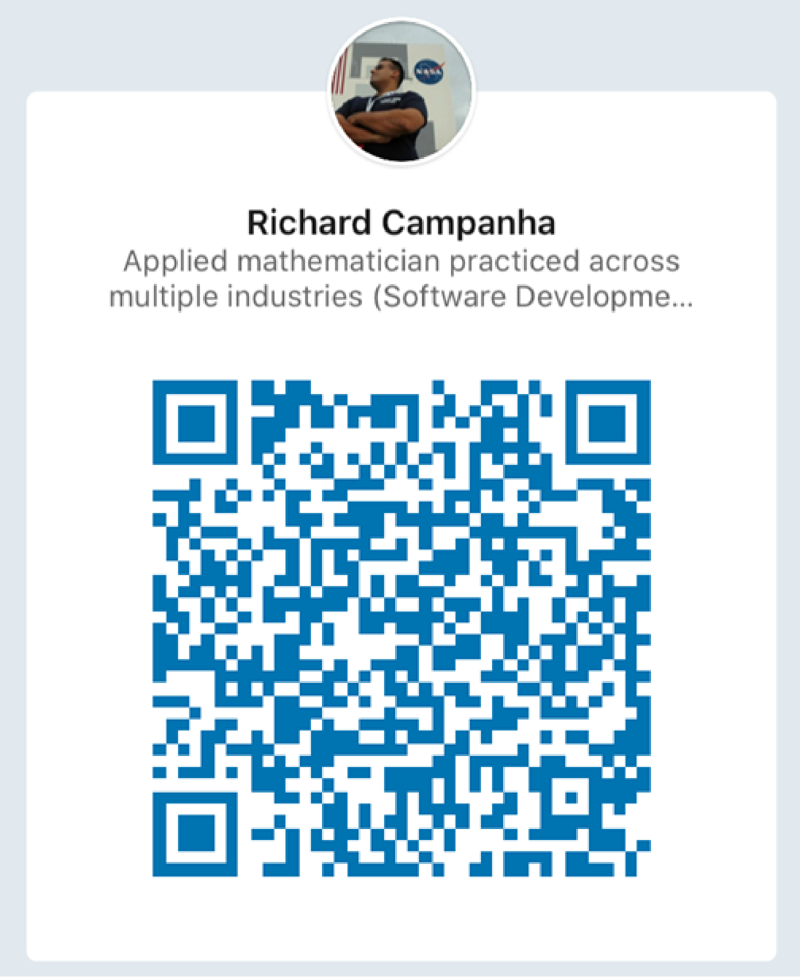
- *2020 may see multiple exploits attacking CVE-2020-0601 (NSA involvement) to deploy malware and ransomware*

- Microsoft – Jan 14th, 2020 announced CVE-2020-0601 (Understood not Aware)
  - Critical Patch announced for Crypt32.dll
  - Allows developers to forge digital certificates to sign software
  - Vulnerable machines can be infected by malware masquerading as digitally signed software
  - Currently in copycat phase, where attackers are reverse engineering the attack (focused on the elliptic curves for signatures)
  - This is likely to accelerate after May 2020 as BTC mining reward halves
  - Recent history shows BTC values begin increasing the year before and continue until the year after a "halvening*" event.
  - Is BTC valuation an incentive for the next potential cyber incident?

- * BTC Halvening means miners receive 50% fewer bitcoins for verifying transactions on the BTC blockchain.

Do Past Incidents Predict the Future?

Questions, Key Take-aways and Contact Information



Richard Campanha
Applied mathematician practiced across multiple industries (Software Developme...

Key Take-aways

Large scale cyber events can *initially* be modelled as pandemic events

Patching exploits, paradoxically, *contributes* to infection rates:

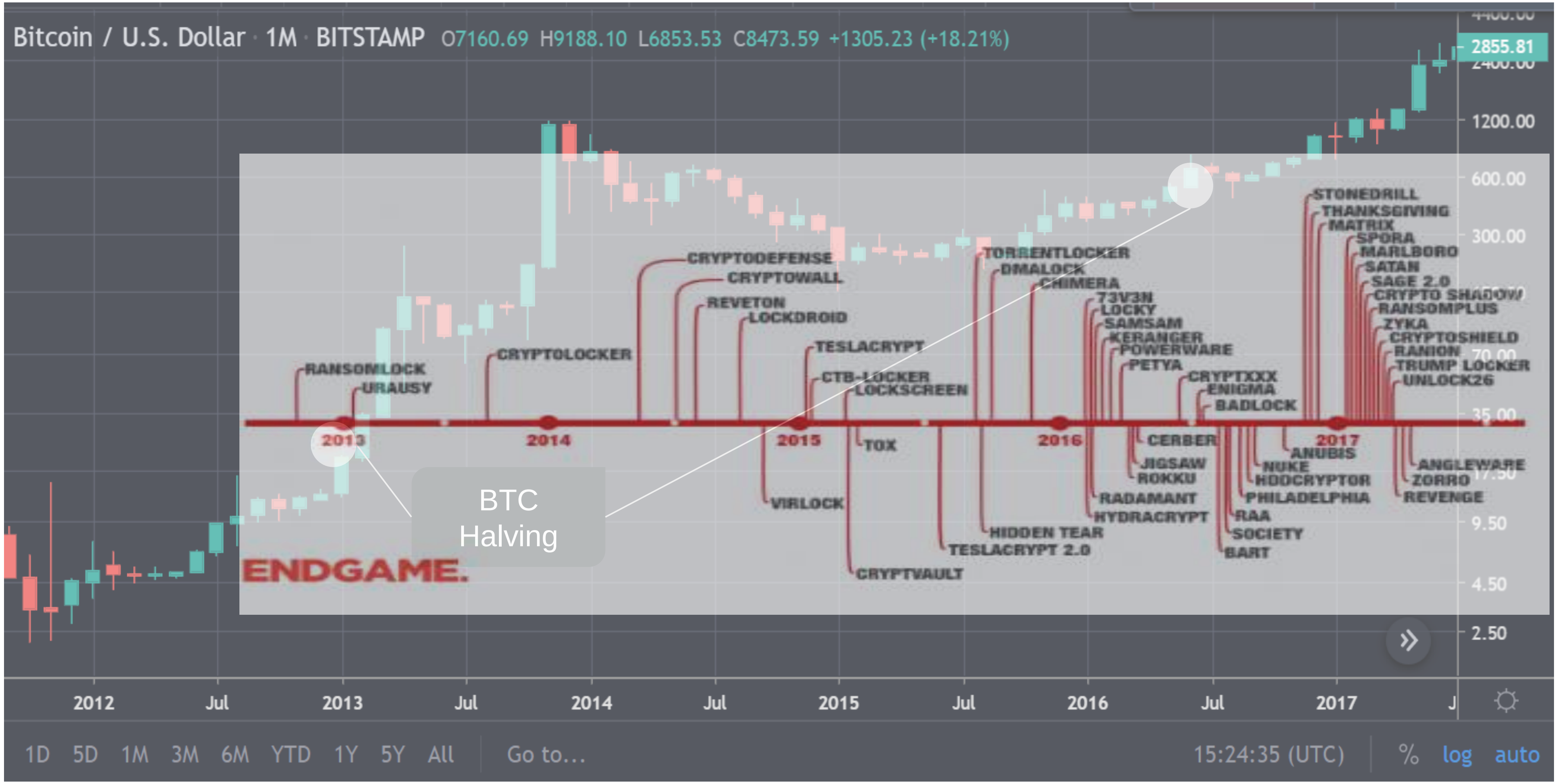
> *This implies a race threshold to cyber modelling large scale events*

Economic incentives can potentially be used to forecast future ransomware events

State attacks should show little correlation to economic metrics and strategic release windows (target nation's holidays)

Appendix

RansomWare Release vs BTC Price



- Breach graph taken from Verizon 2019 Data Breach Investigations Report.
- 50k botnets removed from figure 6 (attributed to External category).
- Bitcoin Chart taken from TradingView.com using BITSTAMP exchange data.

- First BTC Halving Nov 2012
- Second BTC Halving Jul 2016
- Third BTC Halving May 2020

Do Past Incidents Predict the Future?

Questions, Key Take-aways and Contact Information

References

1. https://*darknetdiaries*.com/episode/57/ *(Interview with John Lambert 2020)*
2. https://docs.microsoft.com/en-us/archive/blogs/johnla/*the-inside-story-behind-ms08-067*
3. https://arxiv.org/abs/1603.08307 (Cyber epidemic models)
4. https://www.researchgate.net/publication/315630032_*Mathematical_Model_for_Cyber_Attack_in_Computer_Network*
5. https://nvd.nist.gov/ (CVSS Score)
6. https://www.tradingview.com (Bitstamp data)
7. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
8. https://www.reuters.com/investigates/special-report/usa-spying-raven/
9. *A First Course in Mathematical Modeling*, Giordani, Weir, Fox, Horton, 2008, Cengage Learning
10. https://www.endgame.com/blog/executive-blog/catching-petya-how-endgame-protects-against-another-global-attack

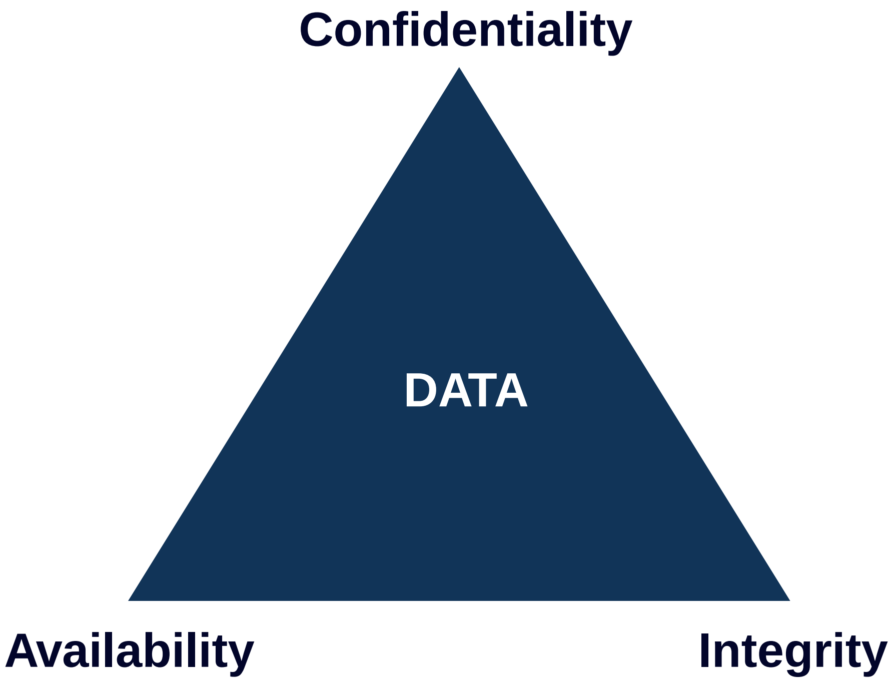
Institute
and Faculty
of Actuaries

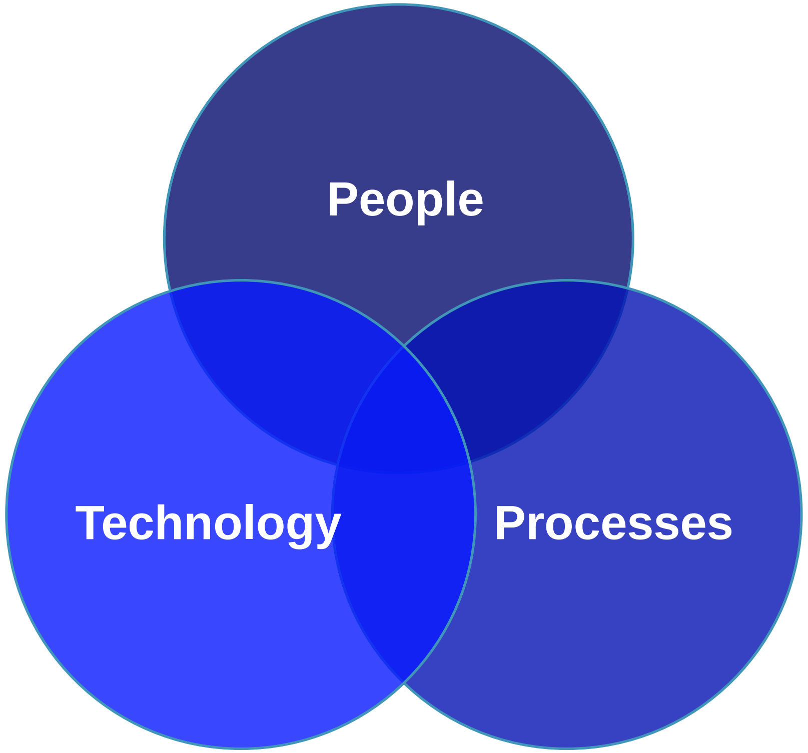
Challenges with quantifying cyber risk

Zoe Mackenzie

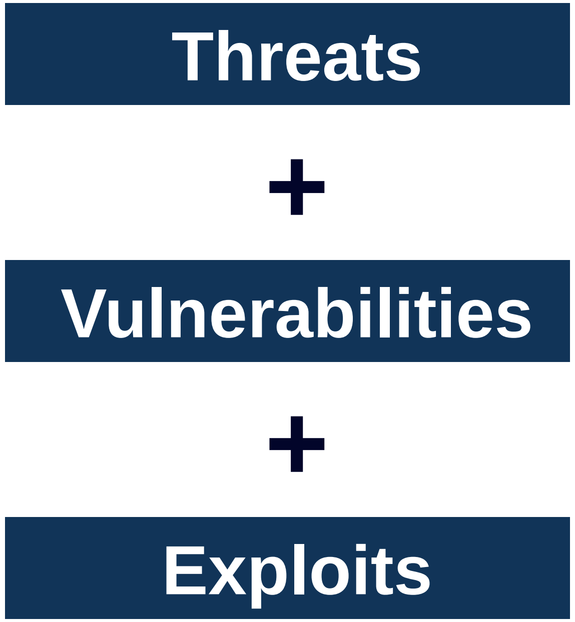
10 February 2020

Cyber Security Principles





Cyber Security Principles



Threats

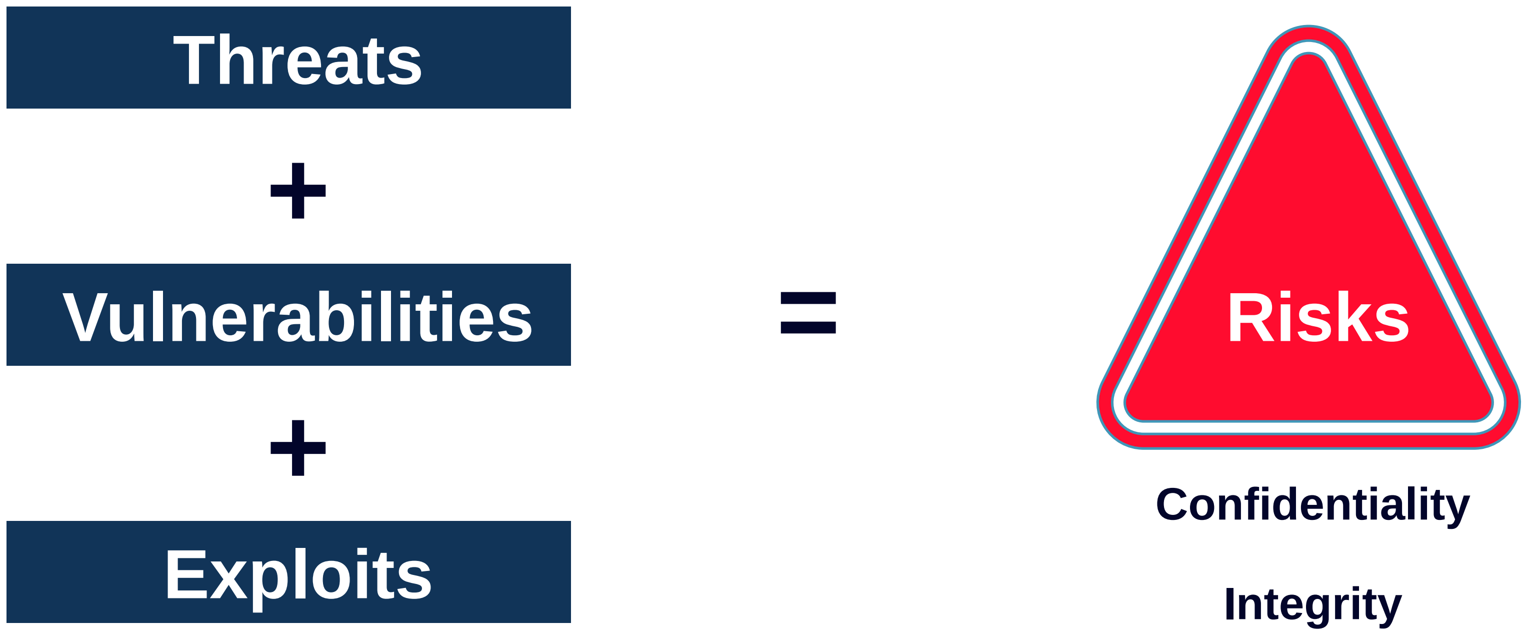
+

Vulnerabilities

+

Exploits

Cyber Security Principles



Threats

+

Vulnerabilities

+

Exploits

=

Risks

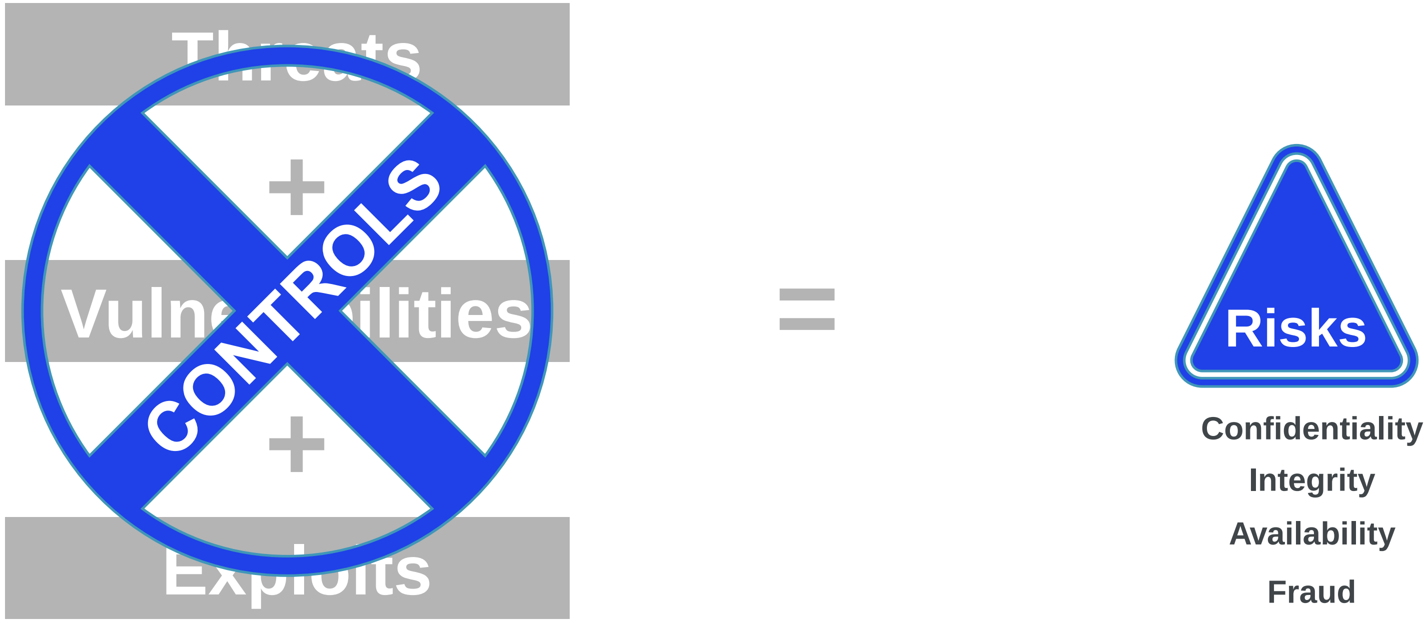
Confidentiality

Integrity

Availability

Fraud

Cyber Security Principles



Confidentiality

Integrity

Availability

Fraud

Risks in more detail

Threats	+	Exploits	+	Vulnerabilities	=	Risks
Cyber Criminals		Phishing + Ransomware		Unpatched Systems		Availability
Nation State		Social Engineering		Poor Training Awareness		Confidentiality
Student		Malicious Computer		Poor Access Control		Integrity

A note to the board…

Cyber criminals could use a phishing email weaponised with ransomware to exploit our unpatched systems, risking the availability of our organisation's network.

CONTROL

Update System Software

Risks in more detail

Threats	+	Exploits	+	Vulnerabilities	=	Risks
Cyber Criminals		Phishing + Ransomware		Unpatched Systems		Availability
Nation State		Social Engineering		Poor Training Awareness		Confidentiality
Student		Malicious Computer		Poor Access Control		Integrity

A note to the board…

A nation state could use social engineering techniques against our staff who have had little security training and awareness, thus risking the confidentiality of our company sensitive data, personal information and intellectual property.

Security Training and Awareness Scheme

Risks in more detail

Threats	+	Exploits	+	Vulnerabilities	=	Risks
Cyber Criminals		Phishing + Ransomware		Unpatched Systems		Availability
Nation State		Social Engineering		Poor Training Awareness		Confidentiality
Student		Malicious Computer		Poor Access Control		Integrity

A note to the board…

A malicious student could use a computer on the university's network to exploit the poor access control on our exam results database, thus risking the integrity of the exam results data.

Strict Access Control

Risks in more detail

Threats	+	Exploits	+	Vulnerabilities	=	Risks
Cyber Criminals		Phishing + Ransomware		Unpatched Systems		Availability
Nation State		Social Engineering		Poor Training Awareness		Confidentiality
Student		Malicious Computer		Poor Access Control		Integrity

Impact x Likelihood = Risk Score

Risks in more detail

Threats	Exploits	Vulnerabilities	Risks	
Cyber Criminals	Phishing + Ransomware	Unpatched Systems	Availability	£££
Nation State	Social Engineering	Poor Training Awareness	Confidentiality	££
Student	Malicious Computer	Poor Access Control	Integrity	£

Risk acceptance level

Identification

Analysis

Evaluation

Assessment

Cyber risk treatment plan

Uncomfortable Truths

We could do everything right and still get hit with a cyber attack.

We cannot invest in everything, risks have to be prioritised.

There could be unintended consequences to board decisions.

Further Resources

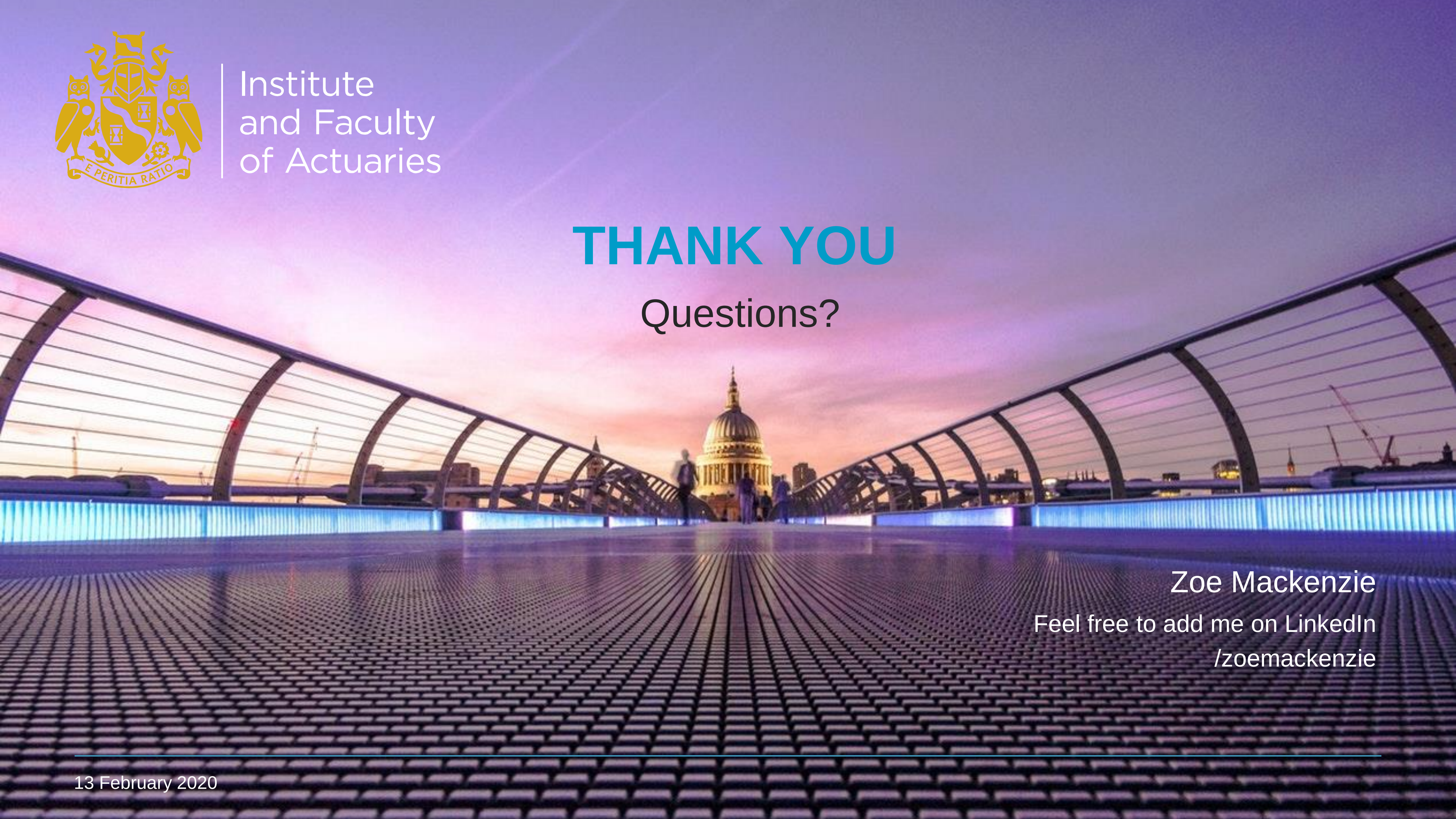
Cyber Body of Knowledge (University of Bristol)
https://www.cybok.org/

Cyber Essentials Framework
https://www.cyberessentials.ncsc.gov.uk/

ISO/IEC 27000 Series Standards
https://www.iso.org/isoiec-27001-information-security.html

NIST Cyber Security Framework
https://www.nist.gov/cyberframework

Centre for Information Security
https://www.cisecurity.org/controls/



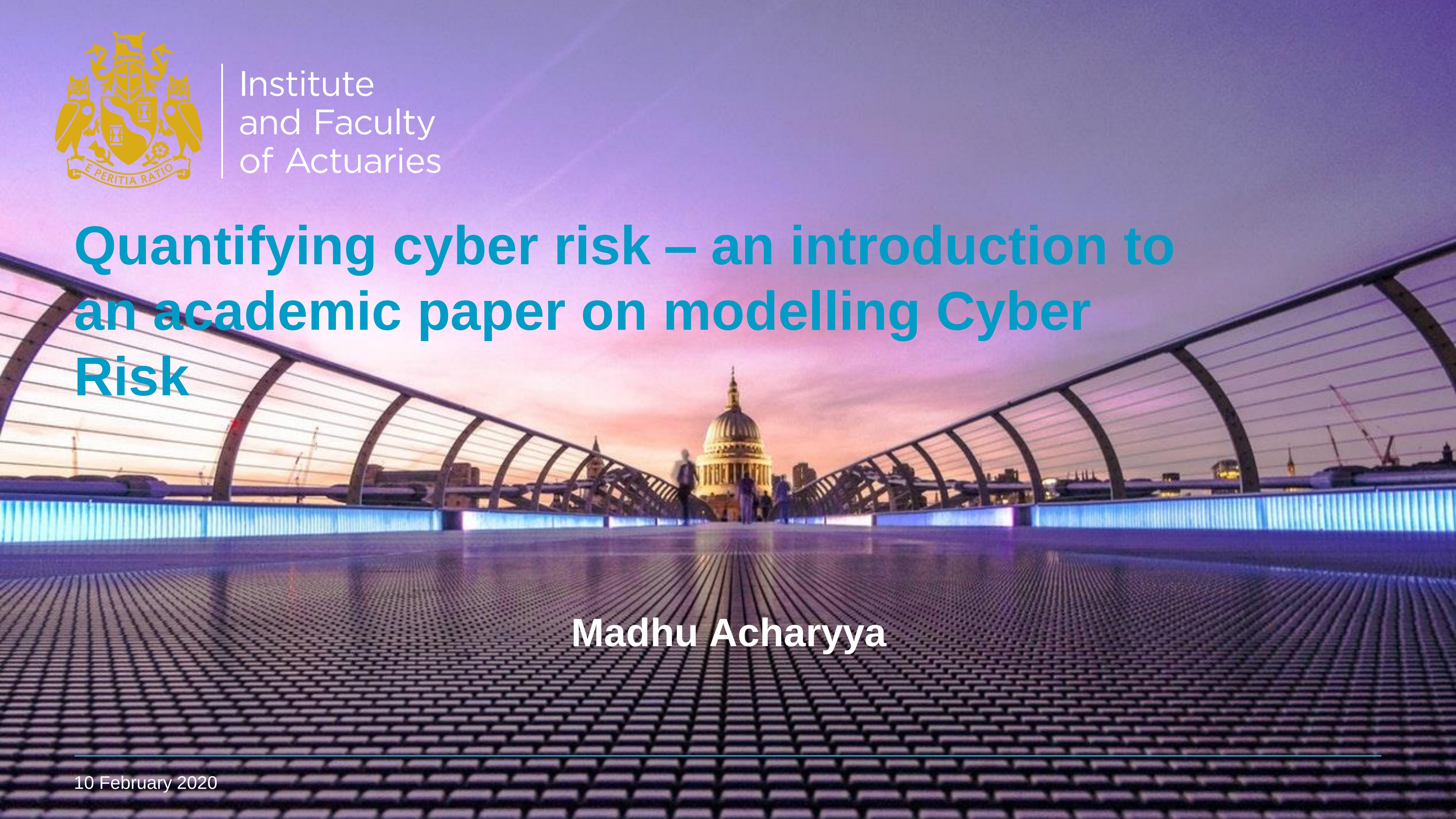
Institute
and Faculty
of Actuaries

THANK YOU

Questions?

Zoe Mackenzie

Feel free to add me on LinkedIn
/zoemackenzie



Institute
and Faculty
of Actuaries

Quantifying cyber risk – an introduction to an academic paper on modelling Cyber Risk

Madhu Acharyya

10 February 2020

Aim & Objectives

- Aim:
  - A Methodology of Quantifying Cyber Risk.

- Objectives:
  - Parameterisation of Cyber Risk
  - Hypothetical Cyber Risk Data
    - LDA
  - Historical Data (4 Case Studies)
  - Aggregate of Loss Distributions
  - Estimation of Capital at Risk (CaR)

Parameters

Parameter Type	No.	Name of Parameters
Category	3	Theft, Damage, Disruption

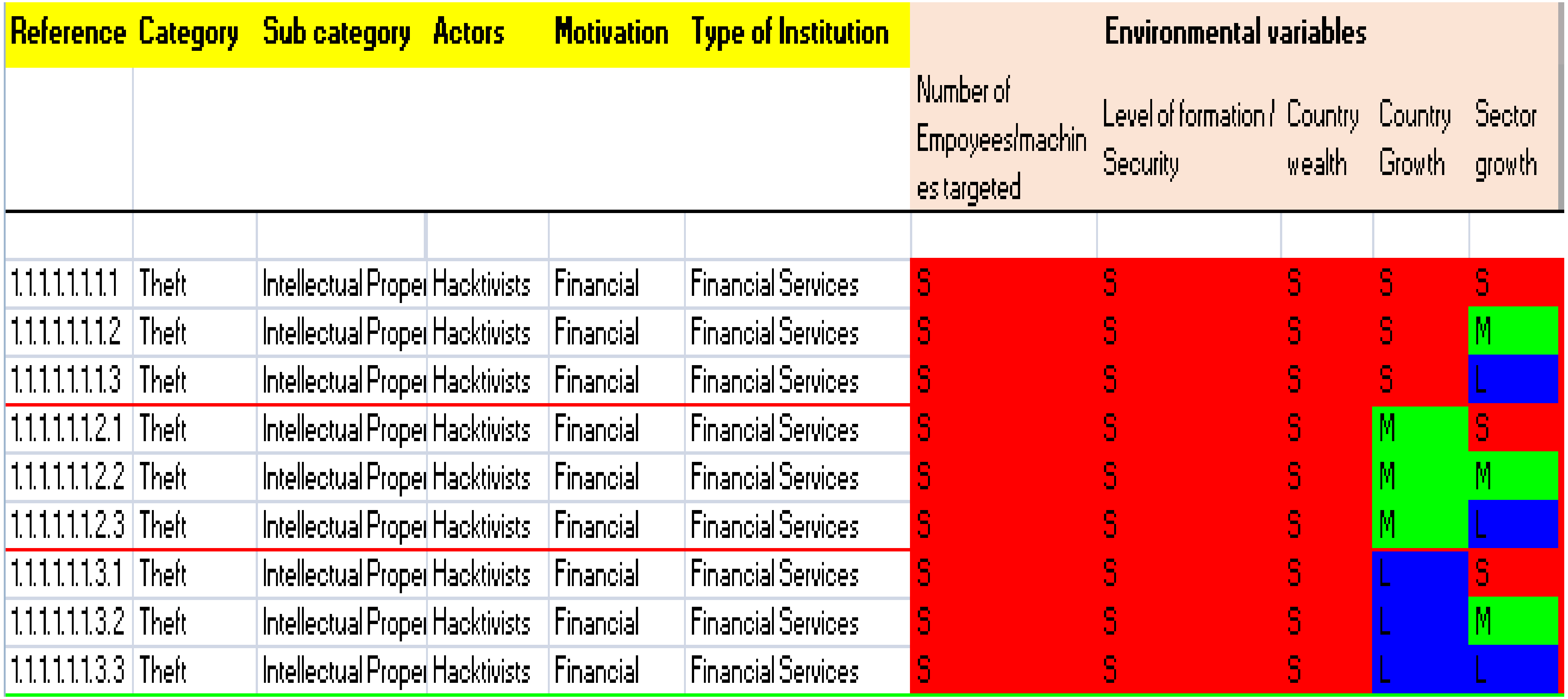
Sub-Category	11	**Data Theft (4):**
		Past (historical), Password or Identity or Credit Card, Intellectual property or Secrets, Money
		Damage (3):
		Amendment or deletion of data; Amendment of algorithm or software; Disable hardware, Hard drive or Server
		Disruption (4):
		Denial of service, Blocking communications, Downtime of websites, Shut down power grid

Actors	4	Hacktivists, Terrorists, Nation state, Lone wolf hackers
Motivations	5	Political, Financial, Social & Cultural, Economic, Personnel
Institution Type	6	Financial Services, Health Care, IT, Entertainment & Media, Retail, Energy
KRI	13	Reputation, % Returning Customers, Clients, MV, Business Interruption, Income Loss, Cost of Service, Property Loss, Financial & Physical Assets, Security, Administrative Expenses, Insurance Expense
Environmental Variables (Factors)	5	Number of Employees and/or Machines targeted, Level of Information (or security), Country Wealth, Country Growth, Sector Growth
Impact Levels	3	Small, Medium, Large

We employed SIX steps methodology to estimate the Impact of Hypothetical Cyber Attack Using LDA

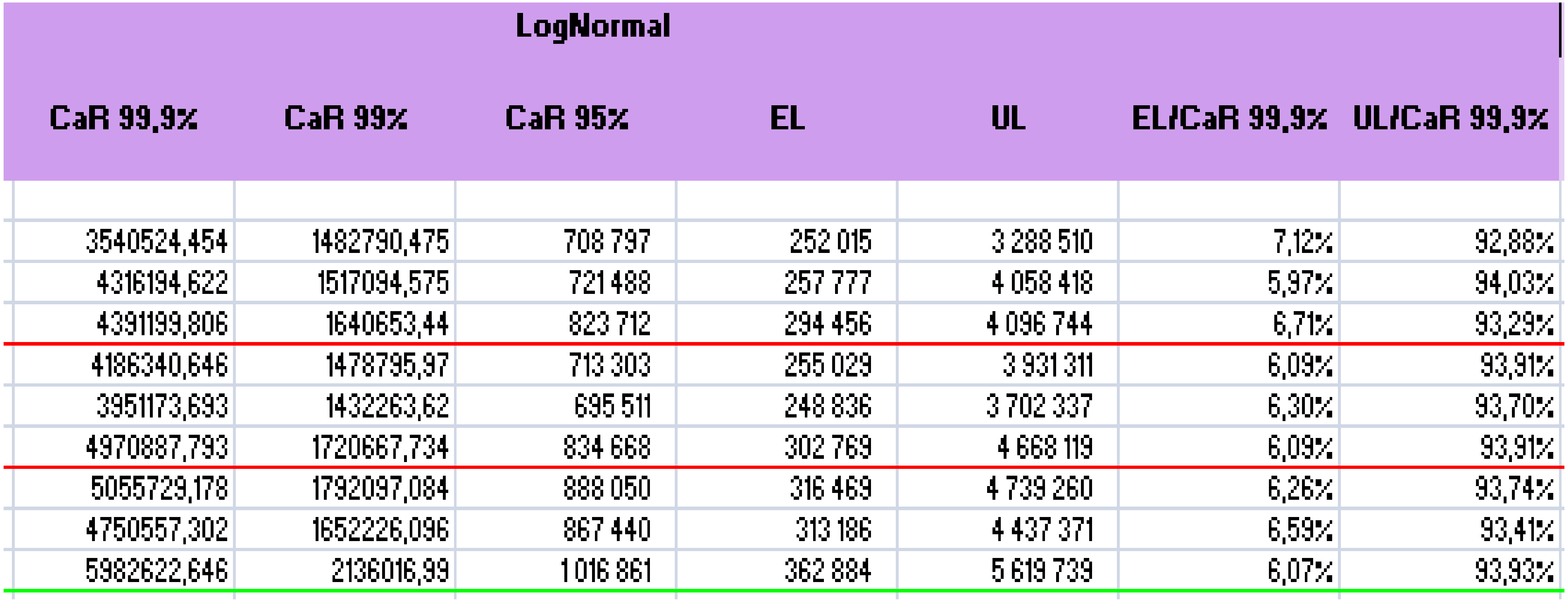
- **Step 1: Computation of Frequency**
- **Step 2: Computation of Severity**
- **Step 3:** Computation of the Impact of the Environmental Variables of the cyber-attacks on the Key Indicators of the Values at Risk
- **Step 5:** Computation of Impact of Cyber Attacks on each of the Values at Risk (4) and of their global impact on the Values at Risk (5)
- **Step 6:** Computation of the Final Severity of Cyber-attacks (6)

Risk Register of Hypothetical Data Generated Through LDA



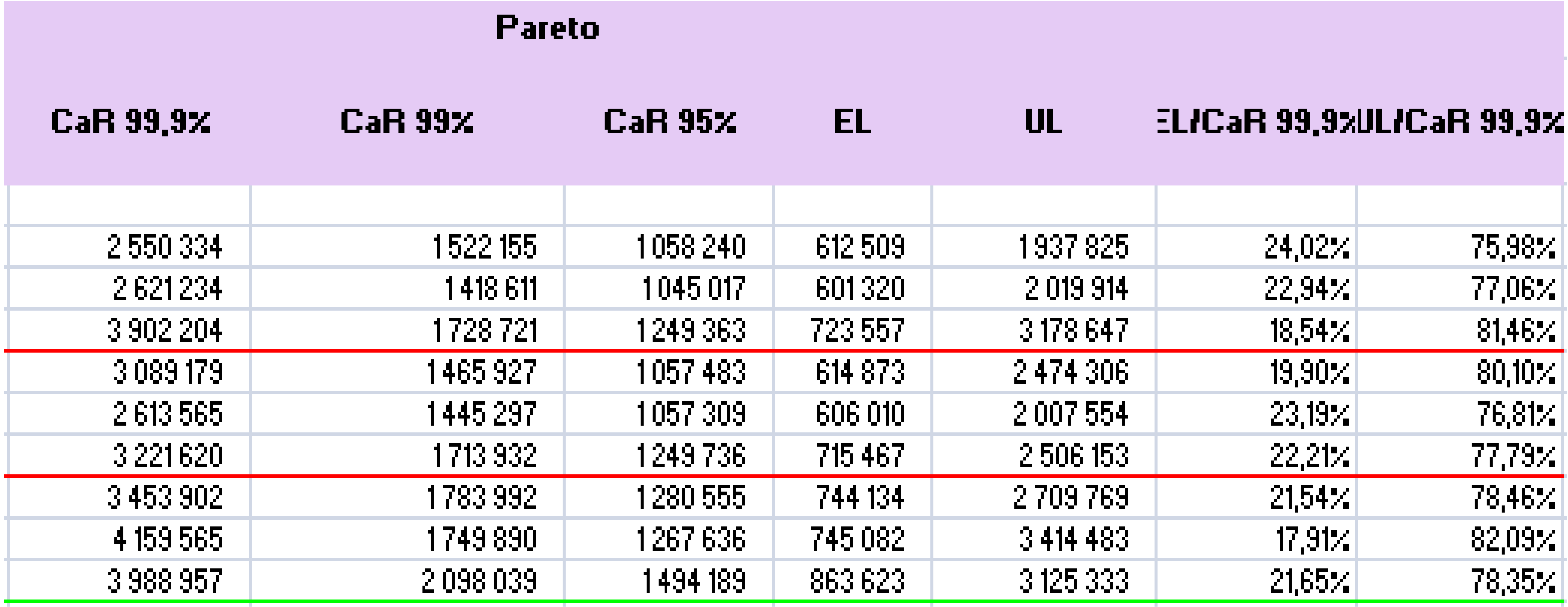
Reference	Category	Sub category	Actors	Motivation	Type of Institution	Environmental variables				
						Number of Empoyees/machines targeted	Level of formation / Security	Country wealth	Country Growth	Sector growth
1.1.1.1.1.1.1.1	Theft	Intellectual Proper	Hacktivists	Financial	Financial Services	S	S	S	S	S
1.1.1.1.1.1.1.2	Theft	Intellectual Proper	Hacktivists	Financial	Financial Services	S	S	S	S	M
1.1.1.1.1.1.1.3	Theft	Intellectual Proper	Hacktivists	Financial	Financial Services	S	S	S	S	L
1.1.1.1.1.1.2.1	Theft	Intellectual Proper	Hacktivists	Financial	Financial Services	S	S	S	M	S
1.1.1.1.1.1.2.2	Theft	Intellectual Proper	Hacktivists	Financial	Financial Services	S	S	S	M	M
1.1.1.1.1.1.2.3	Theft	Intellectual Proper	Hacktivists	Financial	Financial Services	S	S	S	M	L
1.1.1.1.1.1.3.1	Theft	Intellectual Proper	Hacktivists	Financial	Financial Services	S	S	S	L	S
1.1.1.1.1.1.3.2	Theft	Intellectual Proper	Hacktivists	Financial	Financial Services	S	S	S	L	M
1.1.1.1.1.1.3.3	Theft	Intellectual Proper	Hacktivists	Financial	Financial Services	S	S	S	L	L

Aggregate Losses of Hypothetical Data [generated through LDA] Under Scenario 1



LogNormal						
CaR 99,9%	CaR 99%	CaR 95%	EL	UL	EL/CaR 99,9%	UL/CaR 99,9%
3540524,454	1482790,475	708 797	252 015	3 288 510	7,12%	92,88%
4316194,622	1517094,575	721 488	257 777	4 058 418	5,97%	94,03%
4391199,806	1640653,44	823 712	294 456	4 096 744	6,71%	93,29%
4186340,646	1478795,97	713 303	255 029	3 931 311	6,09%	93,91%
3951173,693	1432263,62	695 511	248 836	3 702 337	6,30%	93,70%
4970887,793	1720667,734	834 668	302 769	4 668 119	6,09%	93,91%
5055729,178	1792097,084	888 050	316 469	4 739 260	6,26%	93,74%
4750557,302	1652226,096	867 440	313 186	4 437 371	6,59%	93,41%
5982622,646	2136016,99	1 016 861	362 884	5 619 739	6,07%	93,93%

Aggregate Losses of Hypothetical Data [generated through LDA] Under Scenario 2



Pareto						
CaR 99,9%	CaR 99%	CaR 95%	EL	UL	EL/CaR 99,9%	UL/CaR 99,9%
2 550 334	1 522 155	1 058 240	612 509	1 937 825	24,02%	75,98%
2 621 234	1 418 611	1 045 017	601 320	2 019 914	22,94%	77,06%
3 902 204	1 728 721	1 249 363	723 557	3 178 647	18,54%	81,46%
3 089 179	1 465 927	1 057 483	614 873	2 474 306	19,90%	80,10%
2 613 565	1 445 297	1 057 309	606 010	2 007 554	23,19%	76,81%
3 221 620	1 713 932	1 249 736	715 467	2 506 153	22,21%	77,79%
3 453 902	1 783 992	1 280 555	744 134	2 709 769	21,54%	78,46%
4 159 565	1 749 890	1 267 636	745 082	3 414 483	17,91%	82,09%
3 988 957	2 098 039	1 494 189	863 623	3 125 333	21,65%	78,35%

Case Studies

Bangladesh Bank heist (2016) [near miss loss]	Thieves tried to illegally transfer US$951 million to several fictitious bank accounts around the world	• Weaknesses in the security of the Bangladesh Central Bank • Possible involvement of some of its employees
Sony Pictures hack (2014) Two breaches – 1. a breach of its Playstation network in 2011 2. North Korean attack on its movie studios in 2014	A hacker group which identified itself by the name "Guardians of Peace" (GOP) leaked a release of confidential data from the film studio Sony Pictures.	The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of then-unreleased Sony films, and other information
Talk-Talk (2015) ***Identity theft***	Cyber attack accessed the data of nearly 157,000 customers using a well known hacking technique called SQL injection	A record £400,000 fine by the Information Commissioner’s Office
Anthem (a health insurer) (2015) ***Identity theft***	Criminal hackers had broken into its servers and potentially stolen over 37.5 (later known to 78.8 billion) million records that contain personally identifiable information from its servers	There is fear that the stolen data will be used for identity theft.

http://breachlevelindex.com/data-breach-database

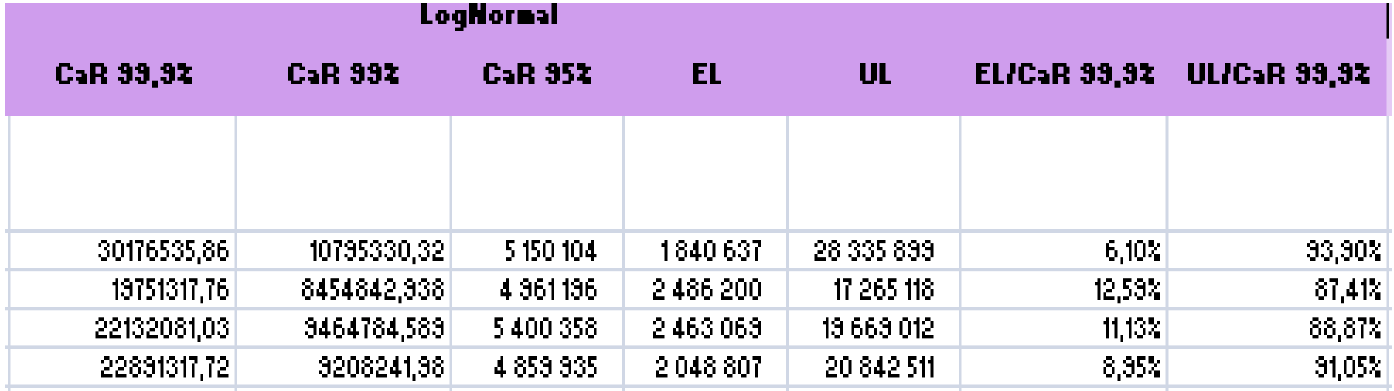
We employed THREE steps methodology to quantify cyber risk from Historical Data

Step 1: Fitting Frequency and Severity Distributions Using Scenario Analysis

Step 2: Generating Aggregate Loss Distributions by Monte Carlo Simulation

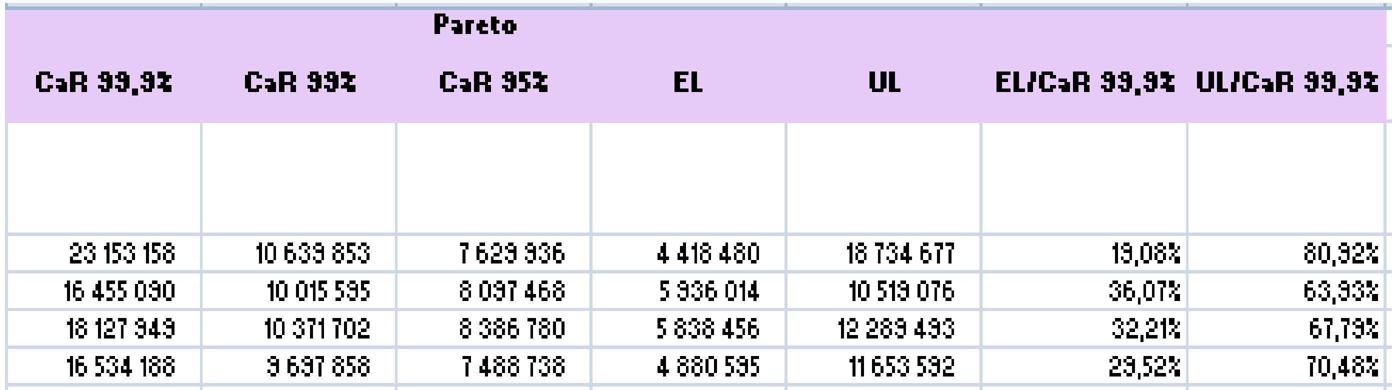
Step 3. Estimation of Capital at Risk (CaR)

Aggregate Losses of Historical Data [Case Studies] Under Scenario 1



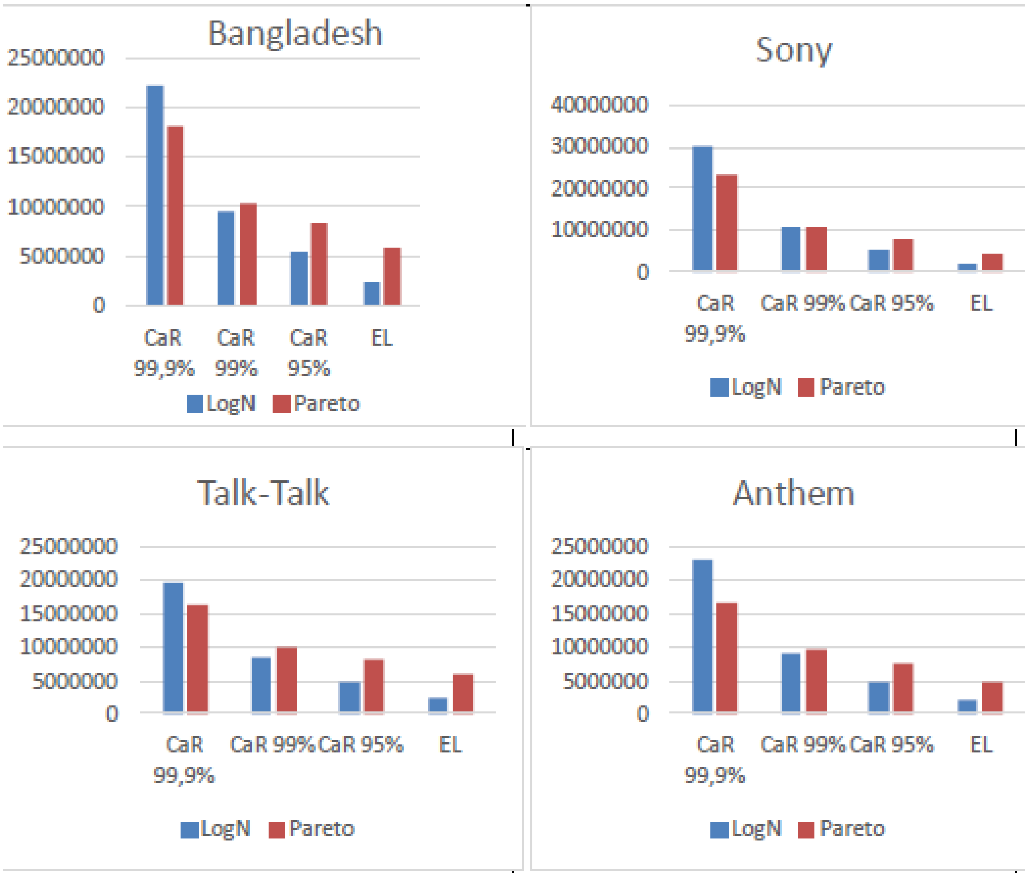
LogNormal						
CaR 99,9%	CaR 99%	CaR 95%	EL	UL	EL/CaR 99,9%	UL/CaR 99,9%
30176535,86	10795330,32	5 150 104	1 840 637	28 335 899	6,10%	93,90%
19751317,76	8454842,938	4 961 196	2 486 200	17 265 118	12,59%	87,41%
22132081,03	9464784,589	5 400 358	2 463 069	19 669 012	11,13%	88,87%
22891317,72	9208241,98	4 859 935	2 048 807	20 842 511	8,95%	91,05%

Aggregate Losses of Historical Data [Case Studies] Under Scenario 2



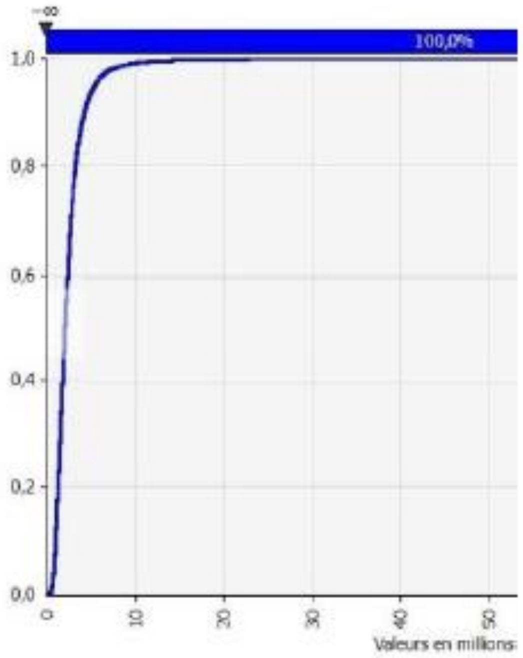
Pareto						
CaR 99,9%	CaR 99%	CaR 95%	EL	UL	EL/CaR 99,9%	UL/CaR 99,9%
23 153 158	10 639 853	7 629 936	4 418 480	18 734 677	19,08%	80,92%
16 455 090	10 015 595	8 097 468	5 936 014	10 519 076	36,07%	63,93%
18 127 949	10 371 702	8 386 780	5 838 456	12 289 493	32,21%	67,79%
16 534 188	9 697 858	7 488 738	4 880 595	11 653 592	29,52%	70,48%

CaR under both Scenarios (Log Normal, Pareto) for the Historical Data

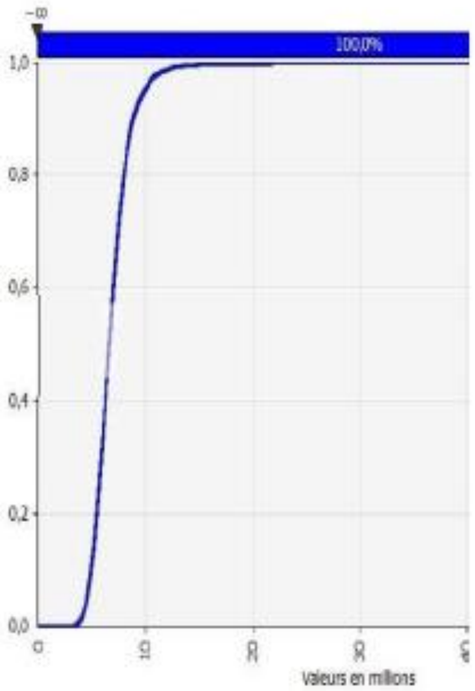


- CaR under both scenarios
- Scenario 1 (Log Normal - in blue) generates lower EL, EL/CaR ratio and higher UL, UL/CaR ratio.
- Although, up to 99% confidence, Scenario 2 (Pareto - in red) generates a higher CaR, at 99,9% confidence, the CaR is slightly smaller for this scenario

CDF under both Scenarios (Log Normal, Pareto) for the Bangladesh Case Study



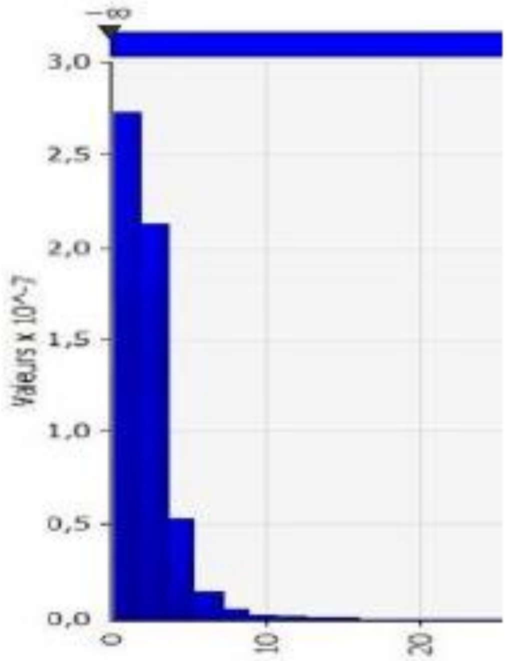
Scenario 1



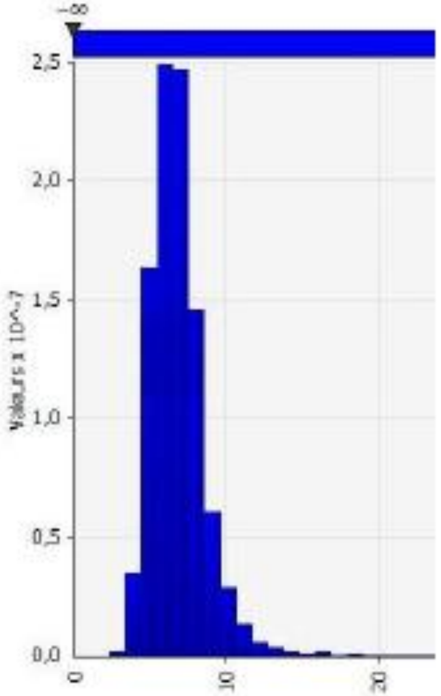
Scenario 2

- 50% of losses under S1 are <3 billions $, under S2, 50% are <7 billions $
- Aggregate loss under S1 are much smaller compared to Under S2
- 50% of the losses under Scenario 1 are below 3 billion $
- whereas 50% of the losses under Scenario 2 are below 7 billion $

PDF under both Scenarios (Log Normal, Pareto) for the Bangladesh case study



Scenario 1



Scenario 1

- 50% of losses under S1 are <3 billions $, under S2, 50% are <7 billions $
- Losses under S1 are concentrated on the left (values are between 0 and 3 billions) whereas in S2 values are between 5*10 billions
- Under S2, smaller UL, CaR Hence, S2 is suitable for risk-averse

Conclusions

- The quantification allows insurers to identify their risk appetite and exposure to cyber risk in order to implement a better measure of cyber risk and pricing of cyber insurance products.
- Although the combination SA/LDA has been previously applied to operational risks, no previous research appeared to have specifically treated the lack of CR data using this method nor creating hypothetical CA
- Will provide a Risk Registrer to capture the data in a comprehensive and systamatic way

Key References

- Biener, C., Eling, M., & Wirfs, J. (2015). "Insurability of Cyber Risk: An Empirical Analysis", Geneva Papers on Risk & Insurance, Vol. 40, pp. 131-158
- Brown, G., & Cox, L. (2011). Making Terrorism Risk Analysis Less Harmful and More Useful: Another Try. Risk Analysis, 31(2), 193-195.
- Cambridge Center for Risk Studies. (2014a). Sybil Logic Bomb Cyber Catastrophe Scenario. Cambridge.
- Cambridge Center for Risk Studies. (2016). Managing Cyber Insurance Accumulation Risk;. Risk Management Solutions.
- Cambridge Centre for Risk Studies. (2014b). Cyber Insurance Exposure Data Schema V1.0. Cambridge, Cyber Accumulation Risk Management Working Paper. Available at http://cambridgeriskframework.com/page/20
- CRO Forum (2014). Cyber Resilience - The cyber risk challenge and the role of insurance. Available at https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-24-1.pdf
- CRO Forum (2016). Concept paper on a proposed categorisation methodology for cyber risk, Available at https://www.thecroforum.org/wp-content/uploads/2016/06/ZRH-16-09033-P1_CRO_Forum_Cyber-Risk_web-2.pdf
- Rodriguez, E., & Dominguez, J. (2008). Scenario analysis for modelling operational losses in the absence of data: the Spanish bank perspective. Journal of Financial Management and Analysis, 21(2), 1-10.
- Swiss Re (2017) "Cyber: getting to grips with a complex risk", Sigma, No. 1. Available at www.swissre.com/sigma
- Swiss Re (2016) "Cyber: in search of resilience in an interconnected world", Swiss Re and IBM joint survey. Available at http://media.swissre.com/documents/ZRH-16-09789-P1_Cyber%20Publication_web1.pdf

- **Dr Madhu Acharyya**
- Senior Lecturer in Risk & Finance, Glasgow Caledonian University, London,
- E-mail: Madhu.Acharyya@gcu.ac.uk

- **Miss Alix Moine**
- Actuarial Sciences Master's Graduate, University of Southampton,
- E-mail: alixmoine@hotmail.com

Institute
and Faculty
of Actuaries

Cyber-Risk: Firms, Individuals and Distributed Resilience Technology

Tiejun Ma

10 February 2020

Cyber-Risk: Firms, Individuals and Distributed Resilience Technology

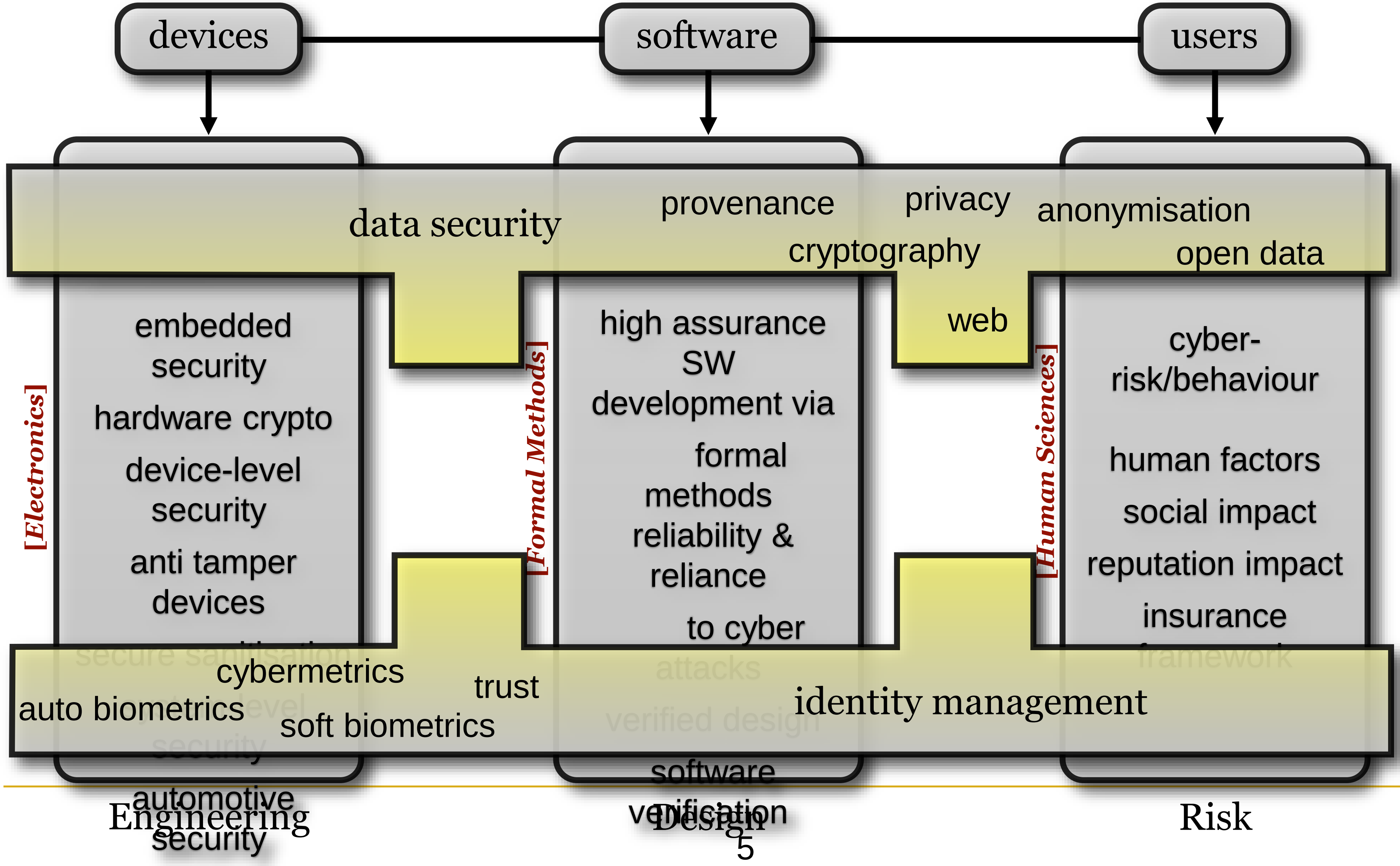
Dr. Tiejun Ma

Associate Professor in Risk Analysis, Centre for Risk Research
Reader in Business Informatics, Artificial Intelligence and Application Institute
Fellow of Alan Turing Institute
Risk Management Research and Thought Leadership Sub-committee, Institute and Faculty of Actuaries

Outline

- **Information**: Sentiment-based cyber-risk quantification
- **Human**: Understanding Individual cyber-risk exposure
- **Technology:** Financial decision making with cyber-risk resilient distributed infrastructure

Cyber-risk where it sits in the landscape



devices

software

users

data security

provenance

privacy

anonymisation

cryptography

open data

web

[Electronics]

embedded security

hardware crypto

device-level security

anti tamper devices

secure sanitisation

device-level security

automotive security

Engineering

[Formal Methods]

high assurance SW development via formal methods reliability & reliance to cyber attacks

verified design

software verification

Design

5

[Human Sciences]

cyber-risk/behaviour

human factors

social impact

reputation impact

insurance framework

Risk

cybermetrics

trust

auto biometrics

soft biometrics

identity management

Case Study: leakage of private customer data to unauthorised users

Data: Time period of study: 2007-2015, Number of events: **84 events** of **52 companies** listed on S&P500

1. Severity of data leakage

Two months after data leakage, each firm loses **1.85%** of market value on average (as shown in Table 1), equivalent to an average loss of **$1.17 billion**

.

➢Consistent with previous studies (Table 2), but suggesting larger losses

Table 1. Average AR on the whole sample

Event month	AR	BMP Z-statistic (p-value)	Percentage of negative value	Sign test Z-statistic (p-value)
t=1	-0.0185 (-1.85%)	-1.9975 (0.0246**)	0.5976	1.7669 (0.0386**)

Table 2. Comparison with results of previous studies

Study	Study period	Sample size	Event window	AR
Liginlala et al. (2009)	2005-2008	151	(-2,9)	-0.59%
Yayla and Hu (2011)	1994-2006	133	(-1,10)	-1.52%
Gatzlaff and McCullough (2010)	2004-2006	77	(0,35)	-1.77%

Institute and Faculty of Actuaries

Case Study: leakage of private customer data to unauthorised users

2. Additional insights into how firm type and event type determine level of loss from data leakage
Privacy sensitive firms suffer more severe impacts, **losing 3.09% or $1.9 billion** of their market value.

Data leakage published on **high-influence media sources** lead to an additional loss of **3.46%** as compared to low-influence sources.

Table 3. Average AR of two sub-samples

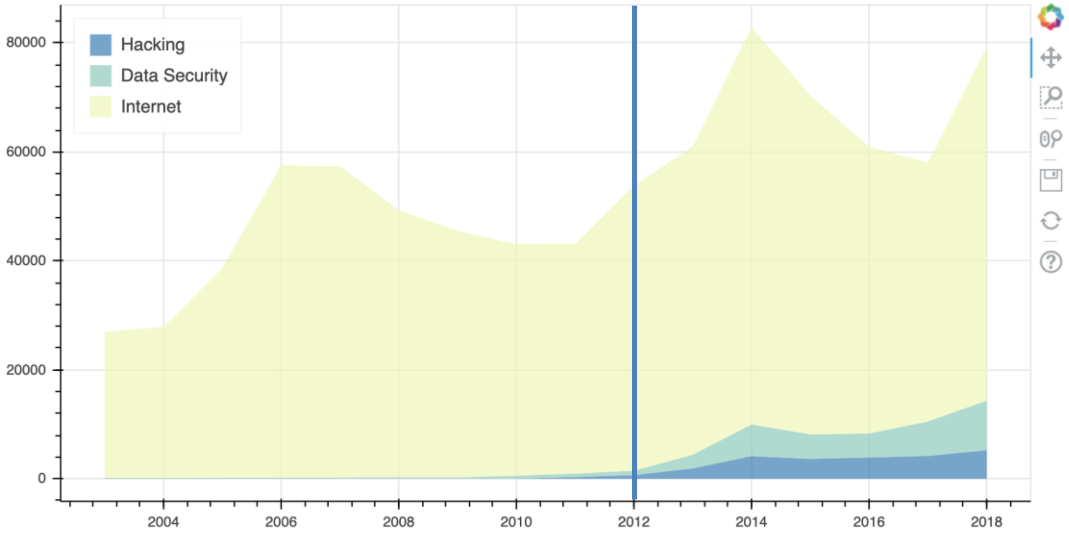
AR	BMP Z-statistic (p-value)	Percentage of negative value	Sign test Z-statistic (p-value)
Privacy sensitive firms			
-0.0309	-3.0312 (0.0012***)	0.7143	2.4424 (0.0073***)
Privacy non-sensitive firms			
-0.0055	-0.0461 (0.4816)	0.4750	-0.4963 (0.6902)

Table 4. Regression analysis

	Coefficient	p-value
Intercept	0.1030	0.3246
Firm size	-0.0046	0.4427
Firm type	-0.0345	0.0127***
Source reach_High	-0.0346	0.0411***
Source reach_Medium	-0.0181	0.2446
Difference in RRI	-5.81E-05	0.9175

- **Privacy sensitive** industry: healthcare, banking and finance firms.

Trend of Cyber-breach Events (35 million news)



Notes: we focus on three types of news. (i) Hacking (Blue): News about computer crime, hacking and cybercrime; (ii) Data Security (Green): News about privacy and data protection; (iii) Internet (Yellow): News about the development in and issues affect the internet. The classification of cyber news is based on the topic codes Reuters use to label news according to its content.

- **The past two decades observed an increase in the amount of cyber event, especially news regarding hacking and data security.**

- The total number of cyber event items increased from 26,954 to 79,310, with a growth rate of nearly 200%.

- Before year 2012, there were little news regarding hacking and data security incidents, but the proportion of these two types of news increased fivefold afterwards, from less than 1‰ to over 5‰.

Cyber Risk Intelligence from Online News

Opportunity

Rich setting to extract and aggregate information

≈ 60% of world population actively communicate via the internet (UN Population Division, 2019)

70% of the UK population above 18 read and download online news (Statista, 2020)

Retrieve real-time information on various risk issues

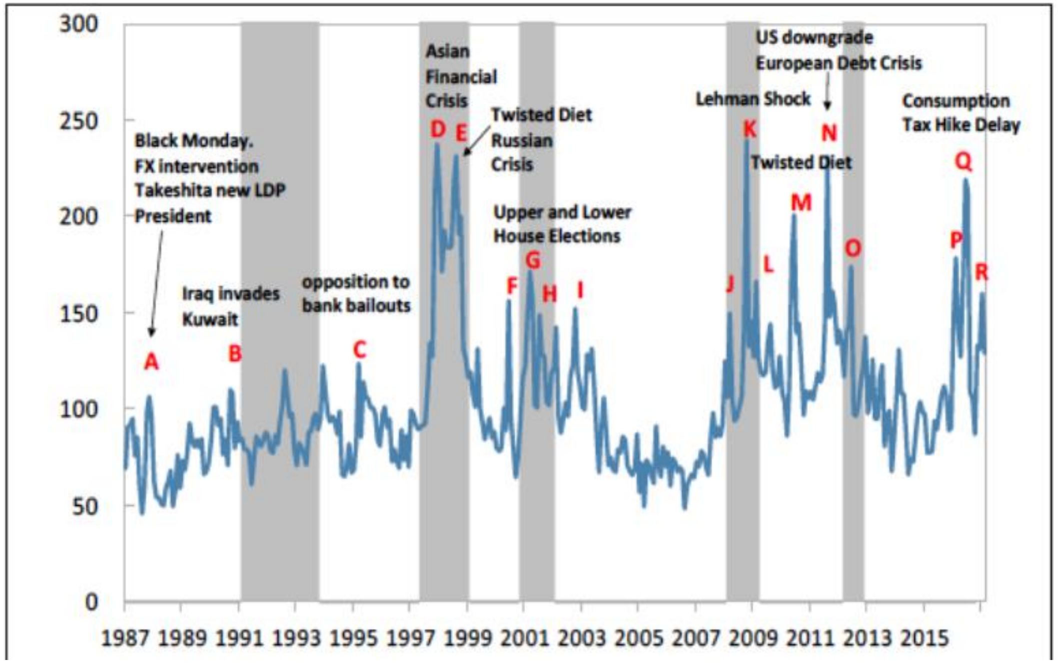
Challenge

Turn qualitative and unstructured text into quantitative and actionable insight

Attribute selection (e.g. Dyer et al., 2017)

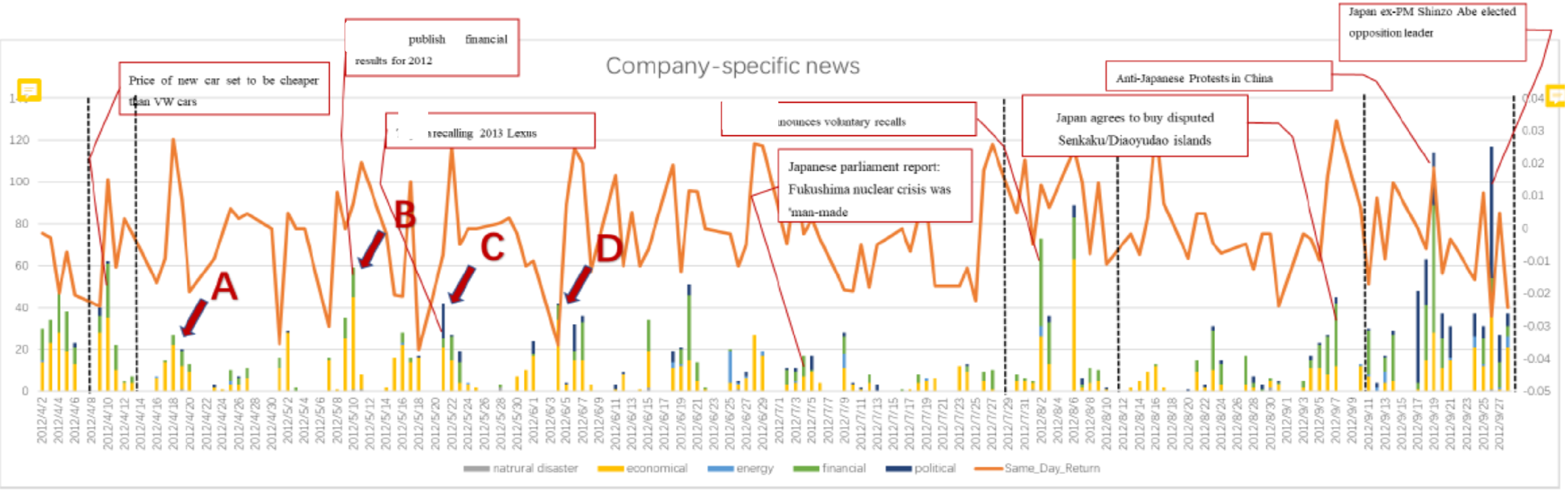
Salience (e.g. Caldara and Iacoviello, 2018)

Semantic attribute (e.g. Tetlock, 2007)



Data and Visualisation

Preliminary analysis – News sentiment score ~ Stock price



Price of new car set to be cheaper than VW cars

publish financial results for 2012

recalling 2013 Lexus

nounces voluntary recalls

Japanese parliament report: Fukushima nuclear crisis was 'man-made

Japan agrees to buy disputed Senkaku/Diaoyudao islands

Anti-Japanese Protests in China

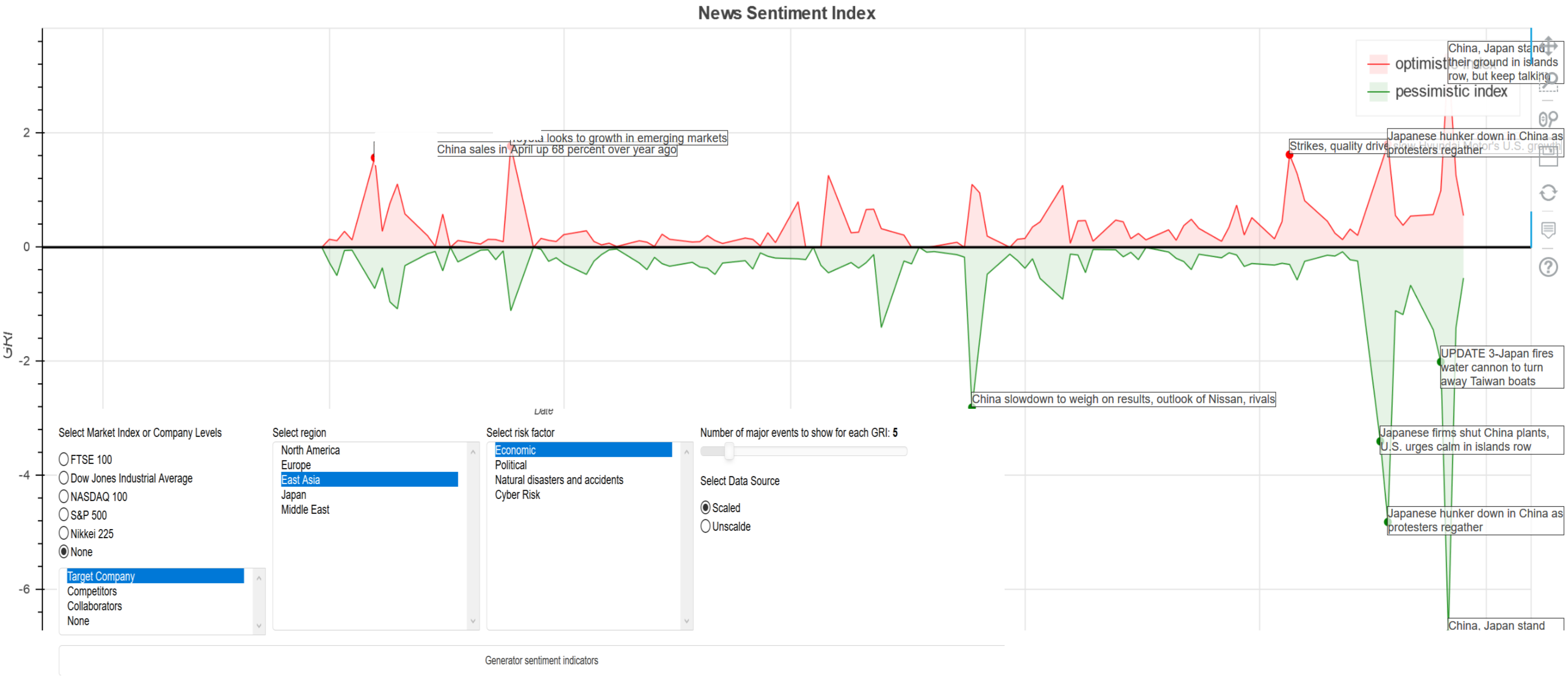
Japan ex-PM Shinzo Abe elected opposition leader

Figure 14 Company level news volume in Japan and return

Note: **Purpose:** to analyse whether the total amount of news of Japan in each trading day has a relationship with the daily return of Toyota stock return; **Legend:** the x-axis represents the date, and each histogram represents the total amount news related to

- *Bar charts: Visualization of the sentiment scores of region factor news*
- *Lines: log return of company stock*

Sentiment Based Cyber Risk Factors Modelling (10million+ news from 8000+ sources)


News Sentiment Index
GRI
2
0
-2
-4
-6
Date
optimistic index
pessimistic index
China sales in April up 68 percent over year ago
Toyota looks to growth in emerging markets
China slowdown to weigh on results, outlook of Nissan, rivals
Strikes, quality drive slow Honda Motor's U.S. growth
Japanese hunker down in China as protesters regather
China, Japan stand their ground in islands row, but keep talking
UPDATE 3-Japan fires water cannon to turn away Taiwan boats
Japanese firms shut China plants, U.S. urges calm in islands row
Japanese hunker down in China as protesters regather
China, Japan stand

Select Market Index or Company Levels

○ FTSE 100
○ Dow Jones Industrial Average
○ NASDAQ 100
○ S&P 500
○ Nikkei 225
● None

[✓ Target Company]
Competitors
Collaborators
None

Select region

North America
Europe
[✓ East Asia]
Japan
Middle East

Select risk factor

[✓ Economic]
Political
Natural disasters and accidents
Cyber Risk

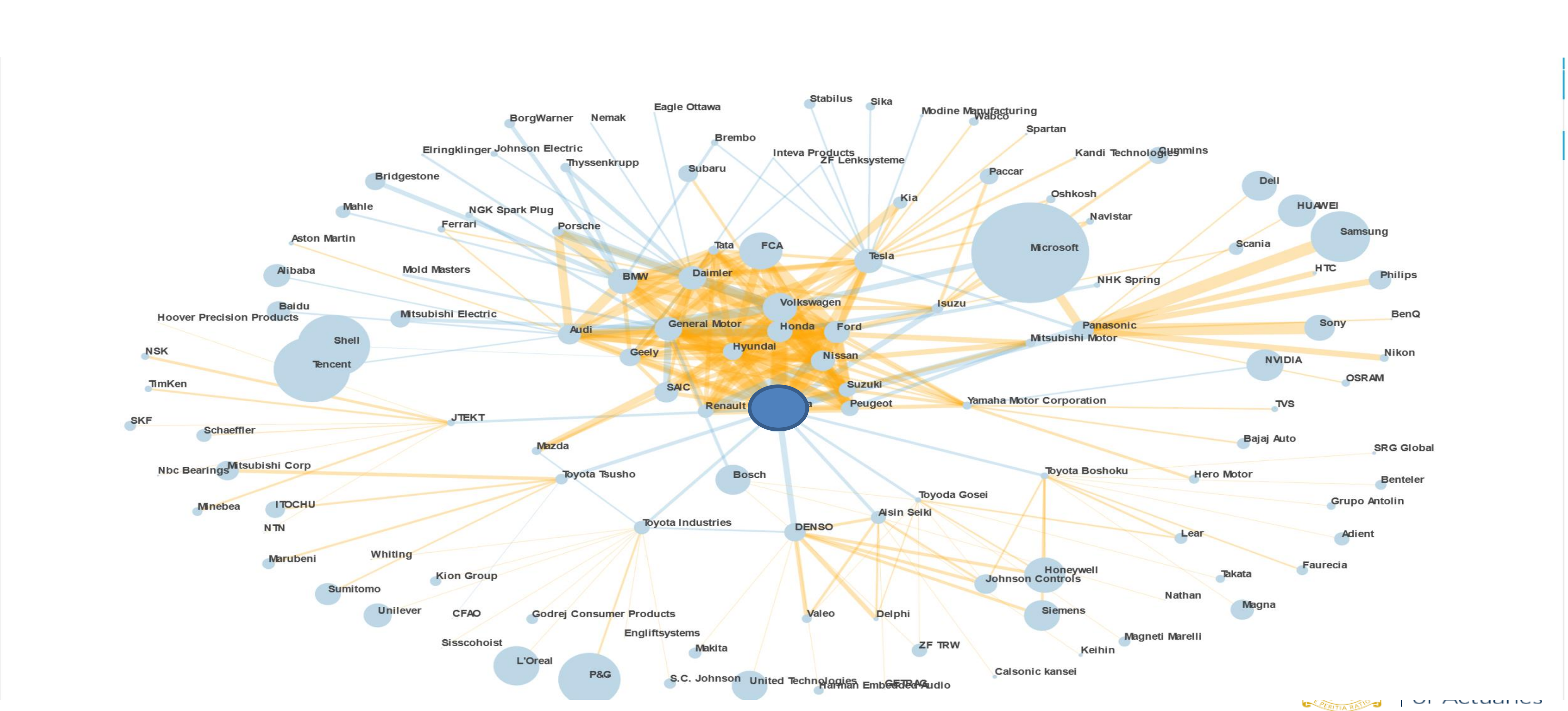
Number of major events to show for each GRI: **5**

Select Data Source

● Scaled
○ Unscalde

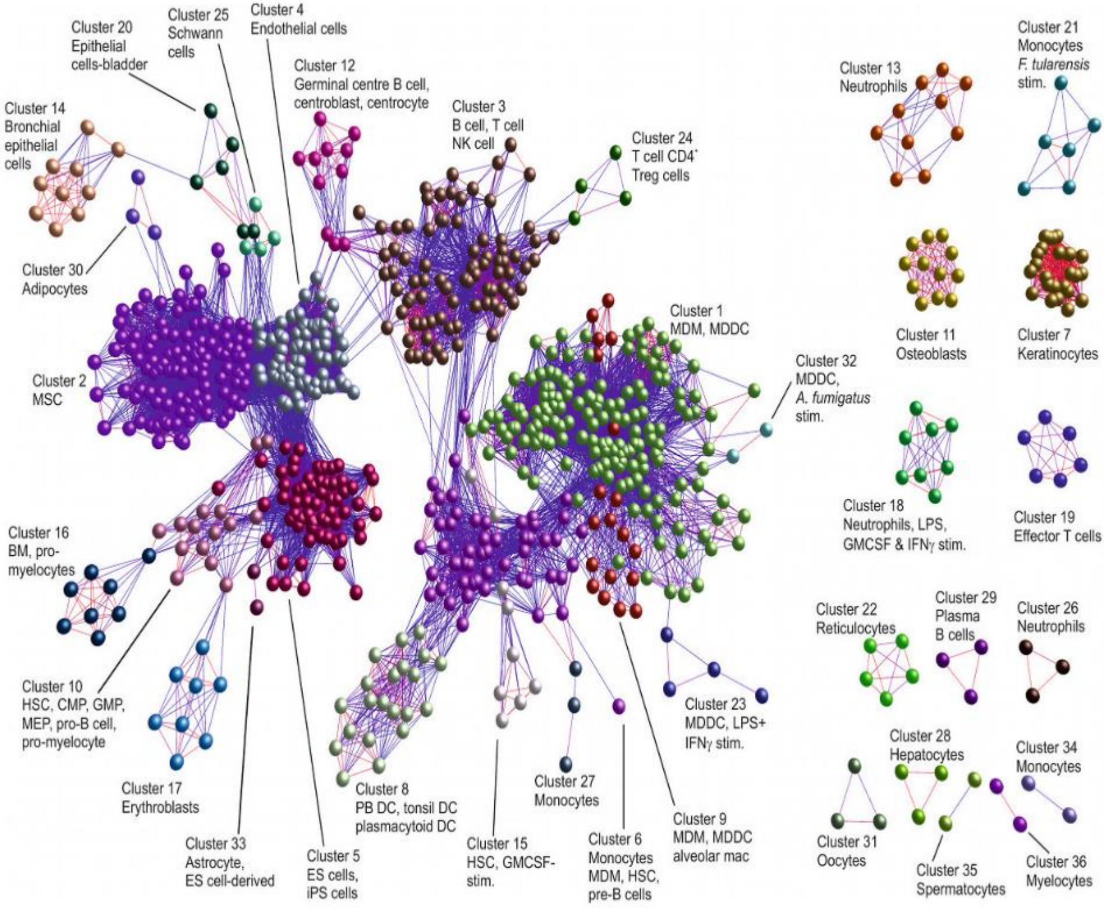
Generator sentiment indicators

Cyber Risk Modelling: Inter-Connected Network



Cyber risk profile

City	Independent variables	B	S.E.	Sig.	Exp(B)
Demographic variables	Gender	-1.007	2.850	.724	.365
	Age	.597	.254	.019	1.817
	Education degree	1.207	1.465	.410	3.344
	Marital status	-3.565	1.718	.038	.028
	Income	1.265	1.062	.234	3.542
	Check-in	2.003	.955	.036	7.415
	Driving licenses	.894	1.597	.575	2.446
Personality	Conscientiousness	-2.932	1.581	.064	.053
	Agreeableness	3.790	1.816	.037	44.278
	Openness	.994	.944	.293	2.701
Risk tolerance	Risk score	-.604	.285	.034	.547
	Constant	-14.850	10.588	.161	.000


Cluster 20 Epithelial cells-bladder
Cluster 25 Schwann cells
Cluster 4 Endothelial cells
Cluster 12 Germinal centre B cell, centroblast, centrocyte
Cluster 14 Bronchial epithelial cells
Cluster 3 B cell, T cell NK cell
Cluster 24 T cell CD4⁺ Treg cells
Cluster 13 Neutrophils
Cluster 21 Monocytes F. tularensis stim.
Cluster 30 Adipocytes
Cluster 2 MSC
Cluster 1 MDM, MDDC
Cluster 32 MDDC, A. fumigatus stim.
Cluster 11 Osteoblasts
Cluster 7 Keratinocytes
Cluster 18 Neutrophils, LPS, GMCSF & IFNγ stim.
Cluster 19 Effector T cells
Cluster 16 BM, pro-myelocytes
Cluster 10 HSC, CMP, GMP, MEP, pro-B cell, pro-myelocyte
Cluster 17 Erythroblasts
Cluster 33 Astrocyte, ES cell-derived
Cluster 5 ES cells, iPS cells
Cluster 8 PB DC, tonsil DC plasmacytoid DC
Cluster 15 HSC, GMCSF-stim.
Cluster 27 Monocytes
Cluster 6 Monocytes MDM, HSC, pre-B cells
Cluster 9 MDM, MDDC alveolar mac
Cluster 23 MDDC, LPS+ IFNγ stim.
Cluster 22 Reticulocytes
Cluster 29 Plasma B cells
Cluster 26 Neutrophils
Cluster 28 Hepatocytes
Cluster 34 Monocytes
Cluster 31 Oocytes
Cluster 35 Spermatocytes
Cluster 36 Myelocytes

Individual Risk Profile

MSc Advanced Technology for Financial Computing
MSc/PhD in Cyber Security, Privacy and Trust

Compulsory modules:

Introduction of Machine Learning
Data Analytics with High Performance Computing
Data-driven Business and Behaviour Analytics

Optional modules:

Algorithmic Game Theory and its Applications
Introduction to Risk Management in Banks
Blockchain and Distributed Ledgers
Text Technologies for Data Science
Data Mining and Exploration

- 4 years PhD Program
- Industry proposed research topic
- Enhanced student's stipends £20k/annum
- Company/Organisation's co-sponsored studentship
- Company contribution 50% of the studentship cost*

Cost to company per studentship £80k* over 4 years (£20k/year)

EDINBURGH
CYBER SECURITY
PRIVACY & TRUST
INSTITUTE

eit Digital

Institute
and Faculty
of Actuaries

*Joining EIT Digital as a member is required (annual membership subscription)

Summary: cross-disciplinary research on risk forecasting, risk taking behaviour, AI-enhanced decision making, and fintech powered cyber risk management.

Dr Tiejun Ma

tiejun.ma@ed.ac.uk

Faculty Fellow of Turing Institute

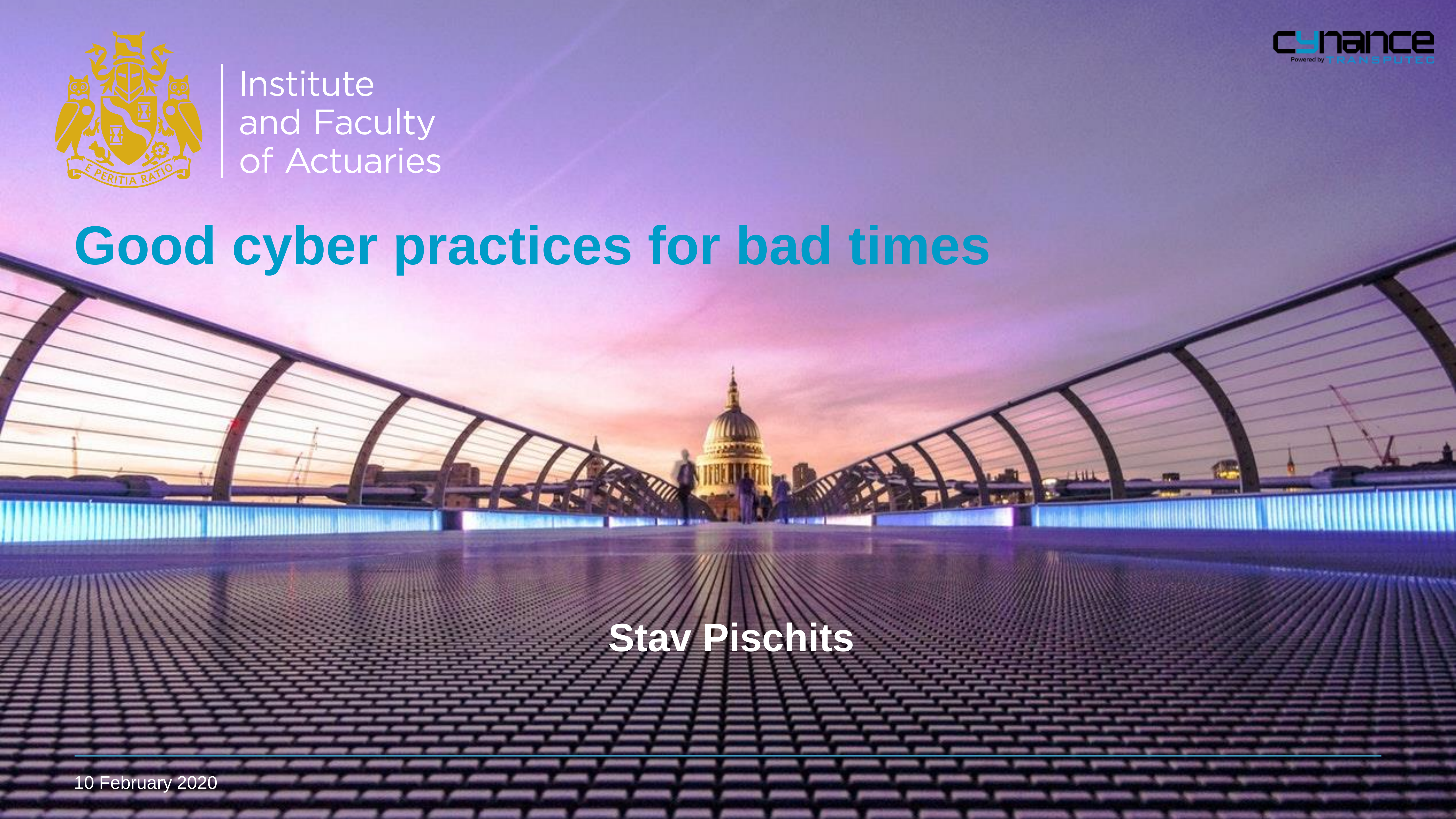
Artificial Intelligence and Applications Institute

The Alan Turing Institute

BayesCentre

THE UNIVERSITY of EDINBURGH informatics

EDINBURGH CYBER SECURITY PRIVACY & TRUST INSTITUTE



Institute and Faculty of Actuaries

cynance
Powered by TRANSPUTEC

Good cyber practices for bad times

Stav Pischits

10 February 2020

Good Cyber Practices for Bad Times

February 2020

Institute
and Faculty
of Actuaries

By cynance
Powered by TRANSPUTEC

About Cynance

Cynance is a cybersecurity and data protection consulting company that was created in order to provide clients with cutting edge information security consulting services, delivered globally

Stav Pischits, CISM, CIPP/E, CPA, MSc.

- Cynance CEO and Co-Founder
- Head of Consulting Operations, Enterprise Security and Incident Response Services Manager @ leading cybersecurity consulting companies
- Information Security Consultant and Project Manager @ big 4 firm
- Counter Terrorism Special Forces
- Cyber Risk Management, Data Protection (GDPR), Cyber Economics, Application Security, Penetration Testing
- Industry Expertise - Finance, Fintech, Gaming, Military Industries

START with y

Why is it so easy to attack you?

Why does your company need cybersecurity?

Why is it so hard to manage cybersecurity?

Why doesn’t your company need to be 100% secure?

CYBERSECURITY VOODOO!

Why is it so easy to attack you?

cynance
Powered by TRANSPUTEC

Hyper Connectivity

PSD2

Wi Fi

aws

DrPrem.com

in

ORACLE

Revolut

SAP

monday.com

slack

zoom

The Modern Days Adversaries

Sophisticated

Motivated

Persistent

Well-Resourced

Stealth

The Attackers

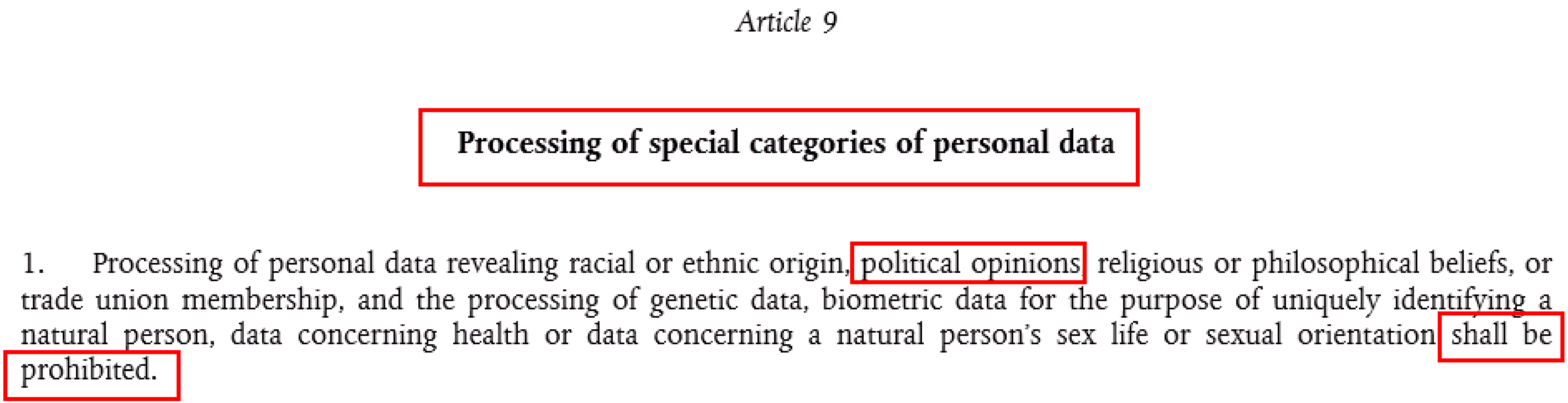
What makes you a hot target?

- You process large amounts of **money**
- You process large amounts of **data**
- You have a good business **reputation**/ too big to fall/ highly **self confident**
- **English** is your first language

cynance

Powered by TRANSPUTEC

Reconnaissance 101

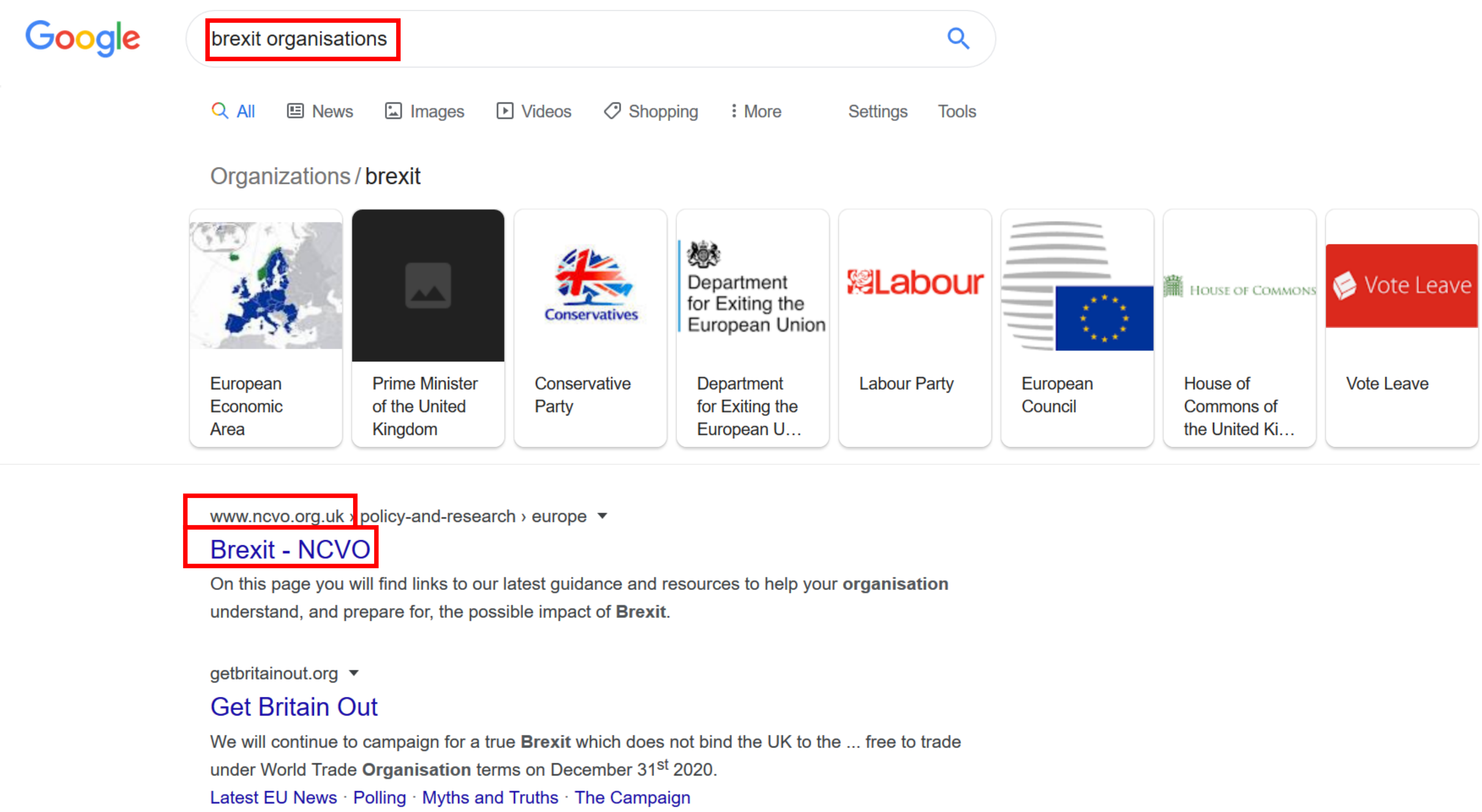


Article 9

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Reconnaissance 101



brexit organisations

Organizations / brexit

European Economic Area · Prime Minister of the United Kingdom · Conservative Party · Department for Exiting the European U… · Labour Party · European Council · House of Commons of the United Ki… · Vote Leave

www.ncvo.org.uk › policy-and-research › europe

Brexit - NCVO

On this page you will find links to our latest guidance and resources to help your **organisation** understand, and prepare for, the possible impact of **Brexit**.

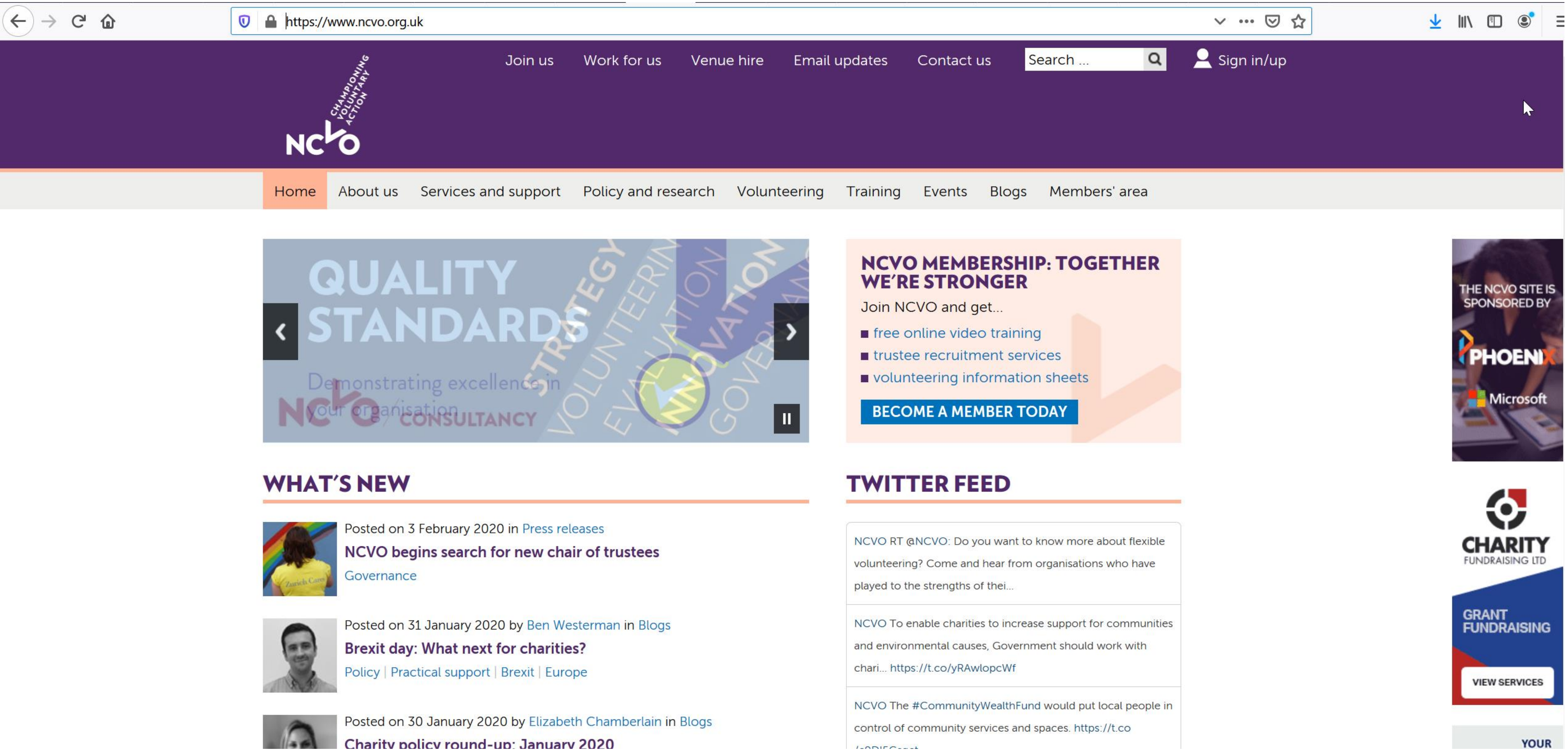
getbritainout.org

Get Britain Out

We will continue to campaign for a true **Brexit** which does not bind the UK to the ... free to trade under World Trade **Organisation** terms on December 31st 2020.

Latest EU News · Polling · Myths and Truths · The Campaign

Reconnaissance 101



NCVO MEMBERSHIP: TOGETHER WE'RE STRONGER

Join NCVO and get...

- free online video training
- trustee recruitment services
- volunteering information sheets

BECOME A MEMBER TODAY

WHAT'S NEW

Posted on 3 February 2020 in Press releases

NCVO begins search for new chair of trustees

Governance

Posted on 31 January 2020 by Ben Westerman in Blogs

Brexit day: What next for charities?

Policy | Practical support | Brexit | Europe

Posted on 30 January 2020 by Elizabeth Chamberlain in Blogs

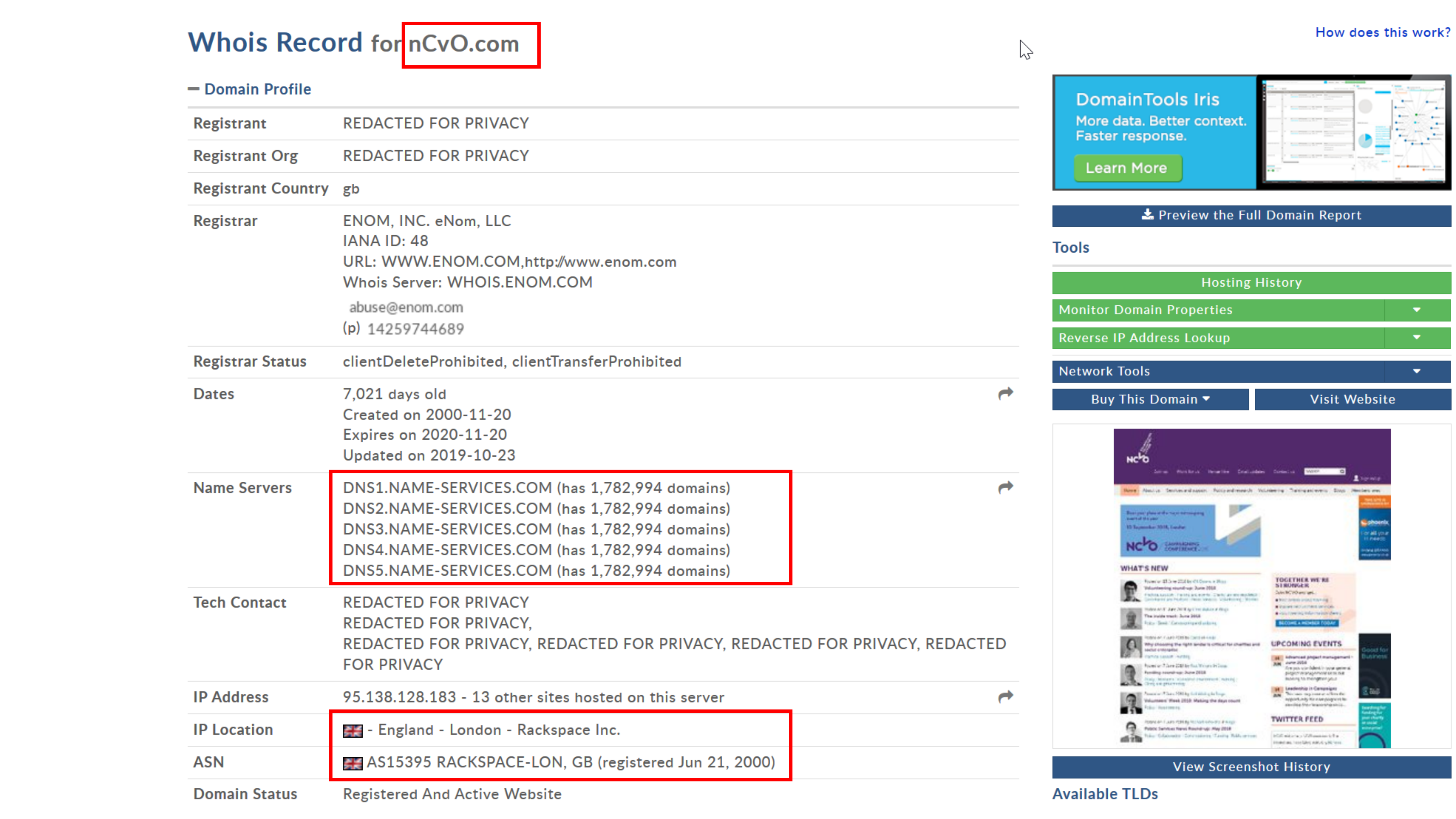
Charity policy round-up: January 2020

TWITTER FEED

NCVO RT @NCVO: Do you want to know more about flexible volunteering? Come and hear from organisations who have played to the strengths of thei...

NCVO To enable charities to increase support for communities and environmental causes, Government should work with chari... https://t.co/yRAwlopcWf

NCVO The #CommunityWealthFund would put local people in control of community services and spaces. https://t.co

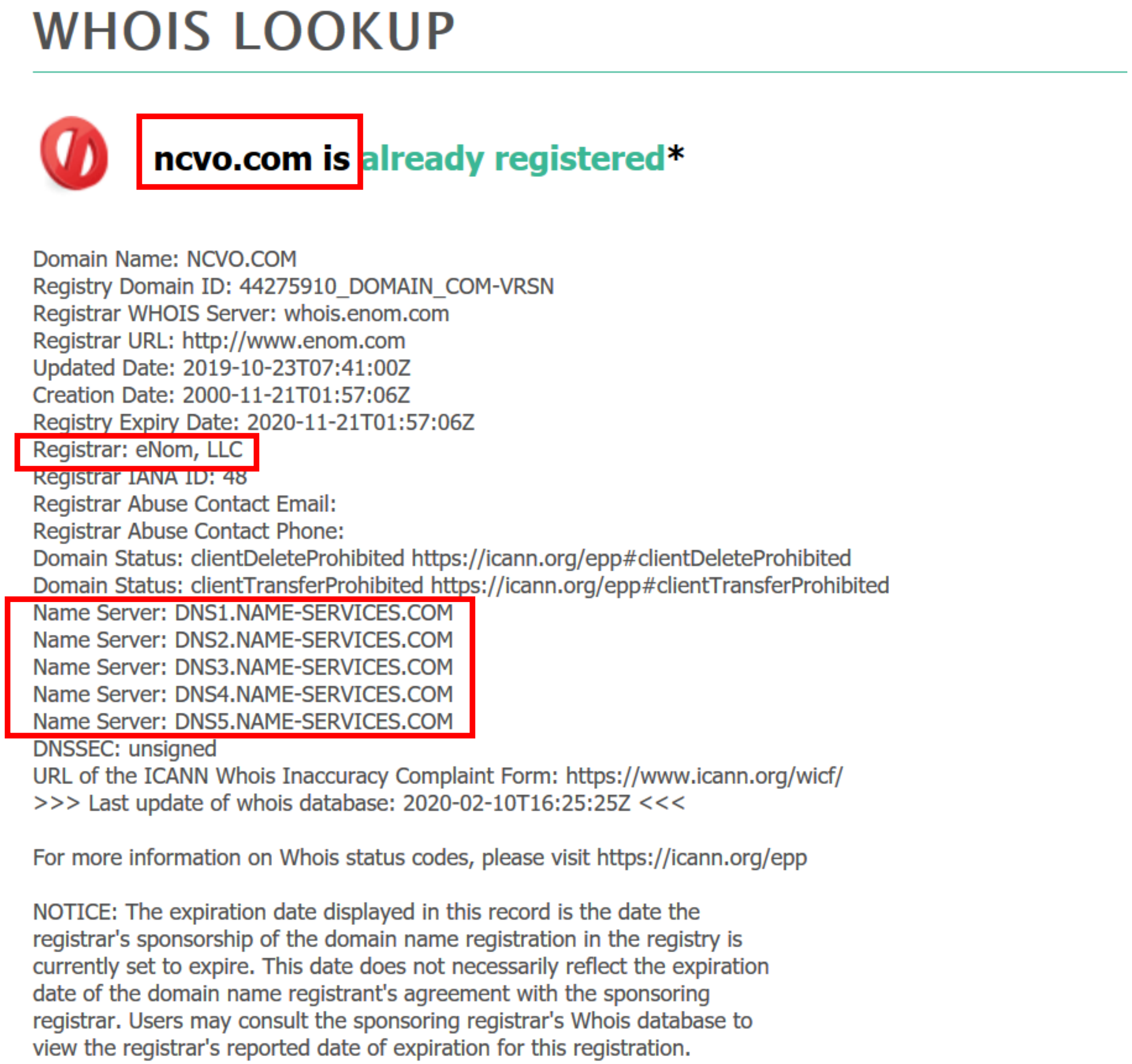


Whois Record for nCvO.com

How does this work?

Domain Profile

Registrant	REDACTED FOR PRIVACY
Registrant Org	REDACTED FOR PRIVACY
Registrant Country	gb
Registrar	ENOM, INC. eNom, LLC IANA ID: 48 URL: WWW.ENOM.COM,http://www.enom.com Whois Server: WHOIS.ENOM.COM abuse@enom.com (p) 14259744689
Registrar Status	clientDeleteProhibited, clientTransferProhibited
Dates	7,021 days old Created on 2000-11-20 Expires on 2020-11-20 Updated on 2019-10-23
Name Servers	DNS1.NAME-SERVICES.COM (has 1,782,994 domains) DNS2.NAME-SERVICES.COM (has 1,782,994 domains) DNS3.NAME-SERVICES.COM (has 1,782,994 domains) DNS4.NAME-SERVICES.COM (has 1,782,994 domains) DNS5.NAME-SERVICES.COM (has 1,782,994 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY
IP Address	95.138.128.183 - 13 other sites hosted on this server
IP Location	🇬🇧 - England - London - Rackspace Inc.
ASN	🇬🇧 AS15395 RACKSPACE-LON, GB (registered Jun 21, 2000)
Domain Status	Registered And Active Website



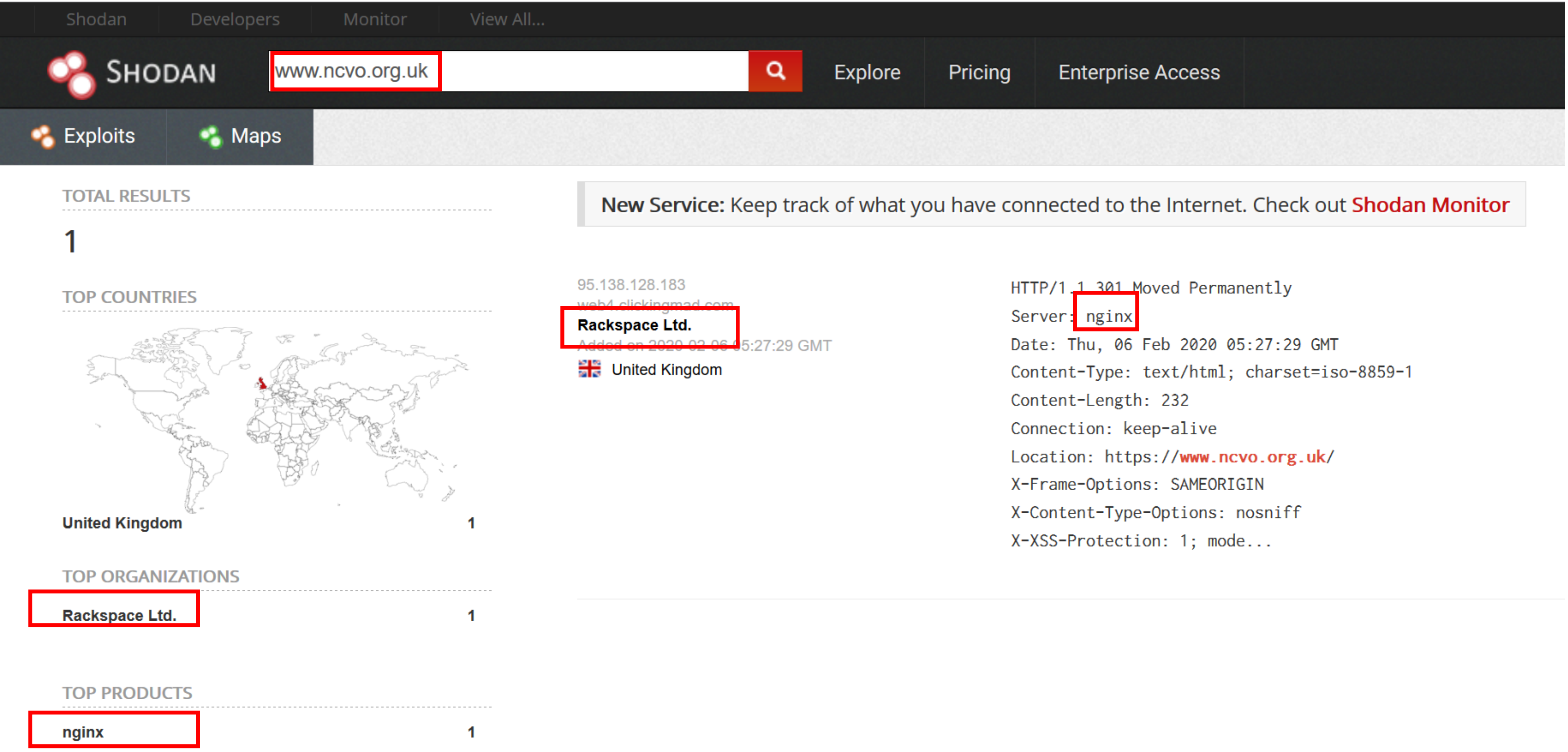
WHOIS LOOKUP

ncvo.com is already registered*

Domain Name: NCVO.COM
Registry Domain ID: 44275910_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.enom.com
Registrar URL: http://www.enom.com
Updated Date: 2019-10-23T07:41:00Z
Creation Date: 2000-11-21T01:57:06Z
Registry Expiry Date: 2020-11-21T01:57:06Z
Registrar: eNom, LLC
Registrar IANA ID: 48
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: DNS1.NAME-SERVICES.COM
Name Server: DNS2.NAME-SERVICES.COM
Name Server: DNS3.NAME-SERVICES.COM
Name Server: DNS4.NAME-SERVICES.COM
Name Server: DNS5.NAME-SERVICES.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-02-10T16:25:25Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.



TOTAL RESULTS

1

TOP COUNTRIES

United Kingdom	1

TOP ORGANIZATIONS

Rackspace Ltd.	1

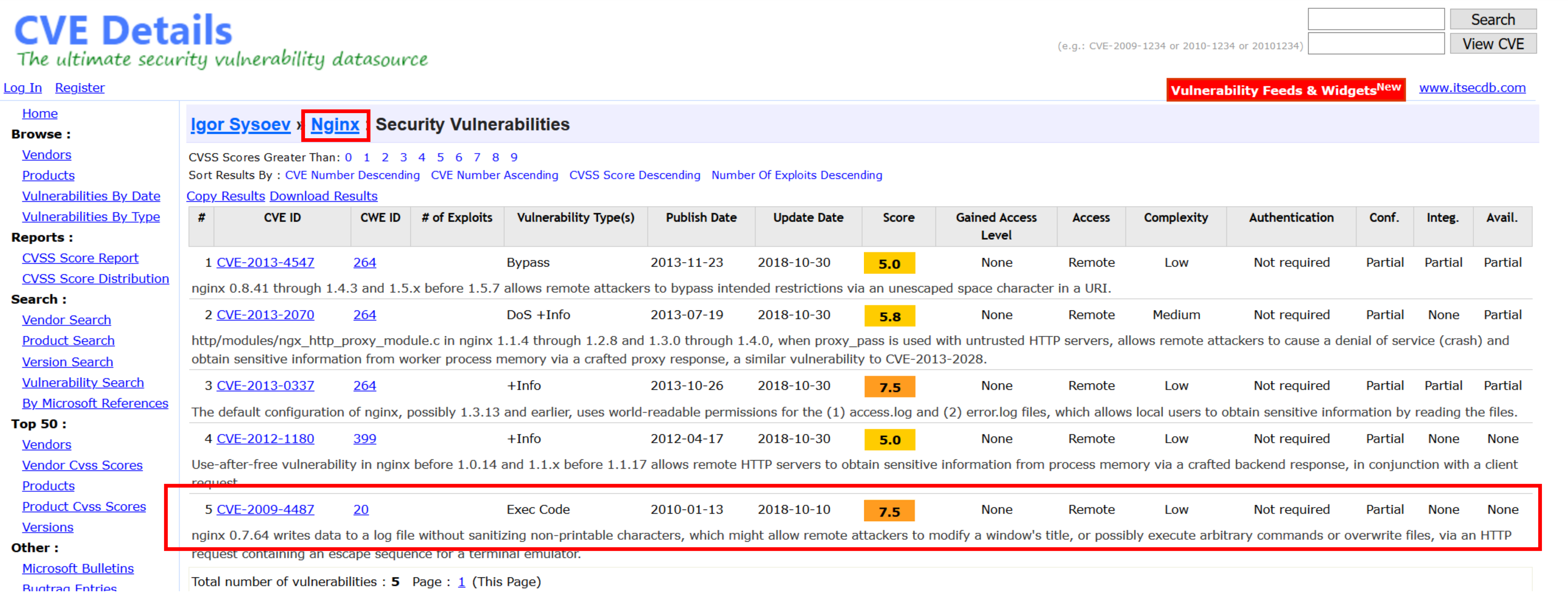
TOP PRODUCTS

nginx	1

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

95.138.128.183
web4.clickingmad.com
Rackspace Ltd.
Added on 2020-02-06 05:27:29 GMT
United Kingdom

```
HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Thu, 06 Feb 2020 05:27:29 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 232
Connection: keep-alive
Location: https://www.ncvo.org.uk/
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode...
```



CVE Details

The ultimate security vulnerability datasource

Search
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
View CVE
Log In
Register
Vulnerability Feeds & WidgetsNew
www.itsecdb.com

- Home

Browse :

- Vendors
- Products
- Vulnerabilities By Date
- Vulnerabilities By Type

Reports :

- CVSS Score Report
- CVSS Score Distribution

Search :

- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :

- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :

- Microsoft Bulletins
- Bugtraq Entries

Igor Sysoev » Nginx : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2013-4547	264		Bypass	2013-11-23	2018-10-30	5.0	None	Remote	Low	Not required	Partial	Partial	Partial
nginx 0.8.41 through 1.4.3 and 1.5.x before 1.5.7 allows remote attackers to bypass intended restrictions via an unescaped space character in a URI.														
2	CVE-2013-2070	264		DoS +Info	2013-07-19	2018-10-30	5.8	None	Remote	Medium	Not required	Partial	None	Partial
http/modules/ngx_http_proxy_module.c in nginx 1.1.4 through 1.2.8 and 1.3.0 through 1.4.0, when proxy_pass is used with untrusted HTTP servers, allows remote attackers to cause a denial of service (crash) and obtain sensitive information from worker process memory via a crafted proxy response, a similar vulnerability to CVE-2013-2028.														
3	CVE-2013-0337	264		+Info	2013-10-26	2018-10-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
The default configuration of nginx, possibly 1.3.13 and earlier, uses world-readable permissions for the (1) access.log and (2) error.log files, which allows local users to obtain sensitive information by reading the files.														
4	CVE-2012-1180	399		+Info	2012-04-17	2018-10-30	5.0	None	Remote	Low	Not required	Partial	None	None
Use-after-free vulnerability in nginx before 1.0.14 and 1.1.x before 1.1.17 allows remote HTTP servers to obtain sensitive information from process memory via a crafted backend response, in conjunction with a client request.														
5	CVE-2009-4487	20		Exec Code	2010-01-13	2018-10-10	7.5	None	Remote	Low	Not required	Partial	None	None
nginx 0.7.64 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.														

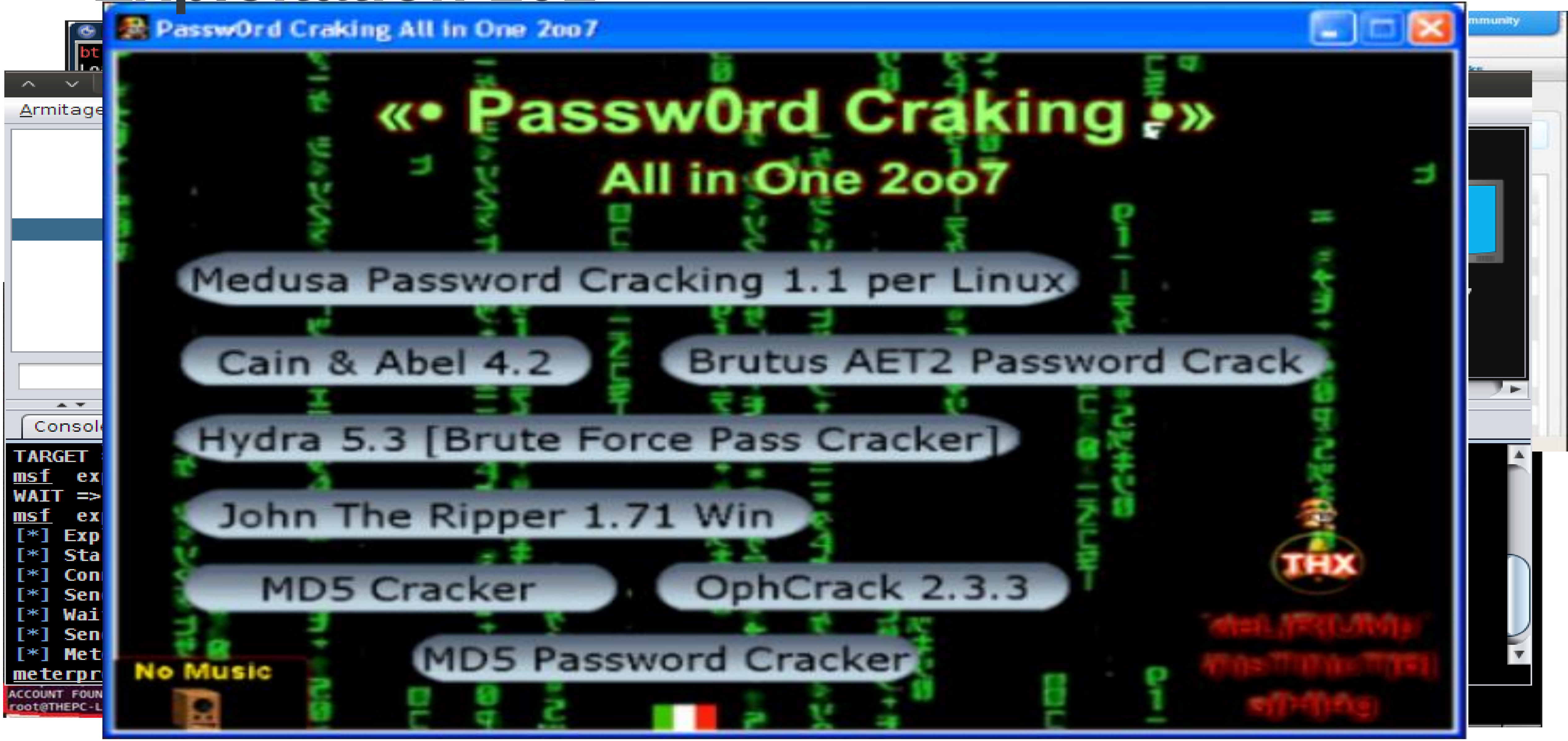
Total number of vulnerabilities : **5** Page : 1 (This Page)

What is a

Remote Code Execution?

A vulnerability that may allow an attacker to run high privileged commands on a server that possesses the appropriate weakness. It may also allow to he attacker to access any and all the information on a server.

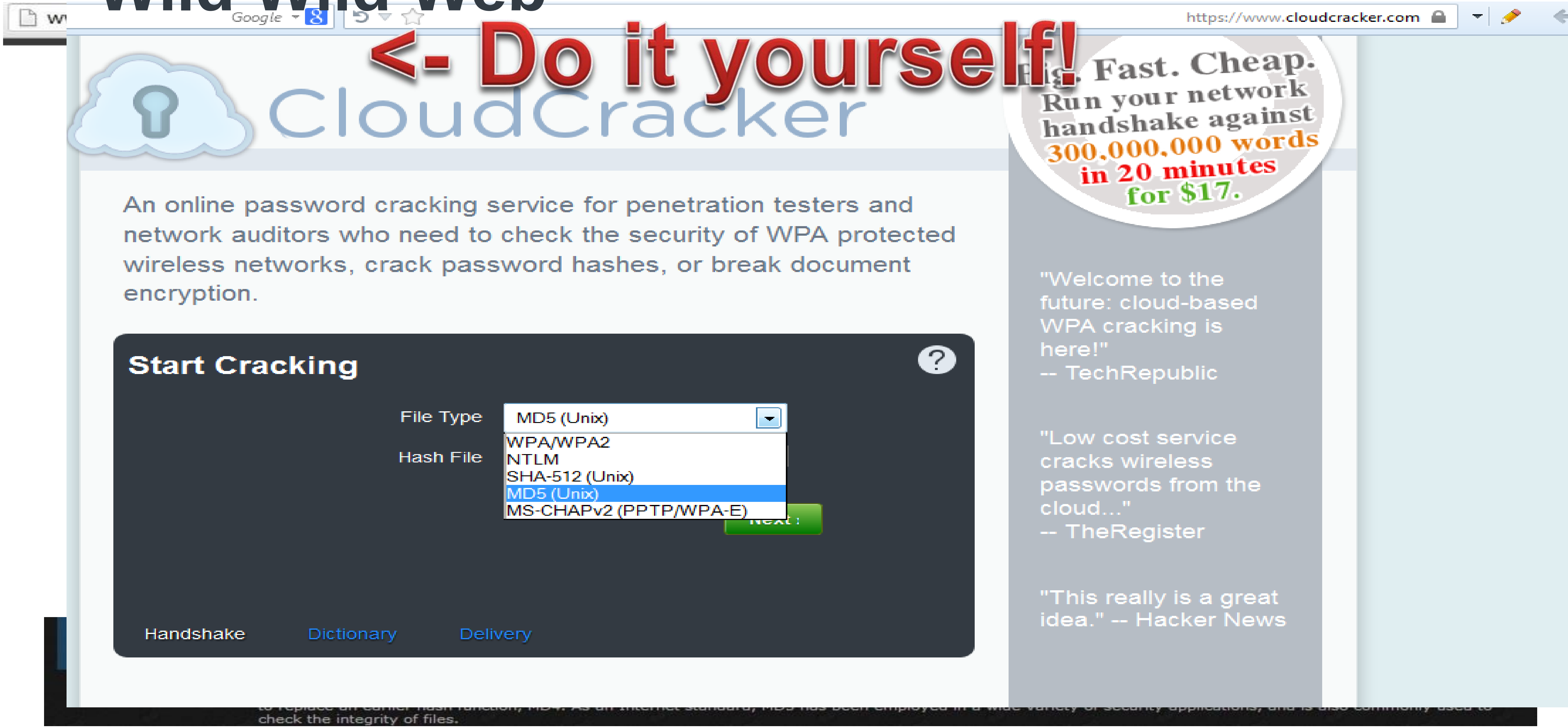
Exploitation 101



```
bt
Lo
```

```
TARGET
msf  ex
WAIT =>
msf  ex
[*] Exp
[*] Sta
[*] Con
[*] Sen
[*] Wai
[*] Sen
[*] Met
meterpr
ACCOUNT FOUN
root@THEPC-L
```

Wild Wild Web



<- Do it yourself!

Big. Fast. Cheap.
Run your network handshake against 300,000,000 words in 20 minutes for $17.

An online password cracking service for penetration testers and network auditors who need to check the security of WPA protected wireless networks, crack password hashes, or break document encryption.

Start Cracking

File Type: MD5 (Unix)

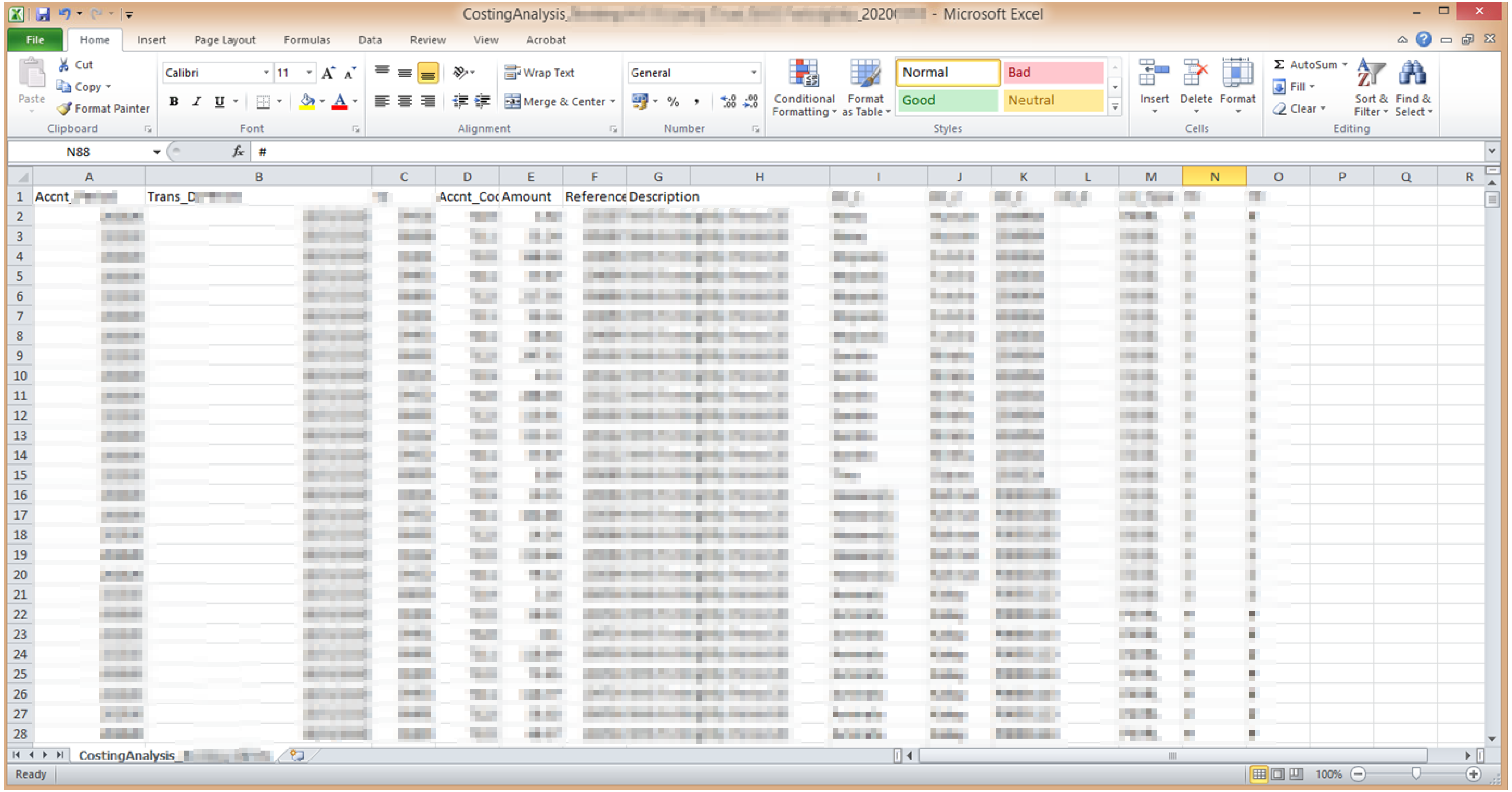
"Welcome to the future: cloud-based WPA cracking is here!"
-- TechRepublic

"Low cost service cracks wireless passwords from the cloud..."
-- TheRegister

"This really is a great idea." -- Hacker News

to replace an earlier hash function, MD4. As an Internet standard, MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files.

BOOOOOOOOOM!



CostingAnalysis_[redacted]_2020[redacted] - Microsoft Excel

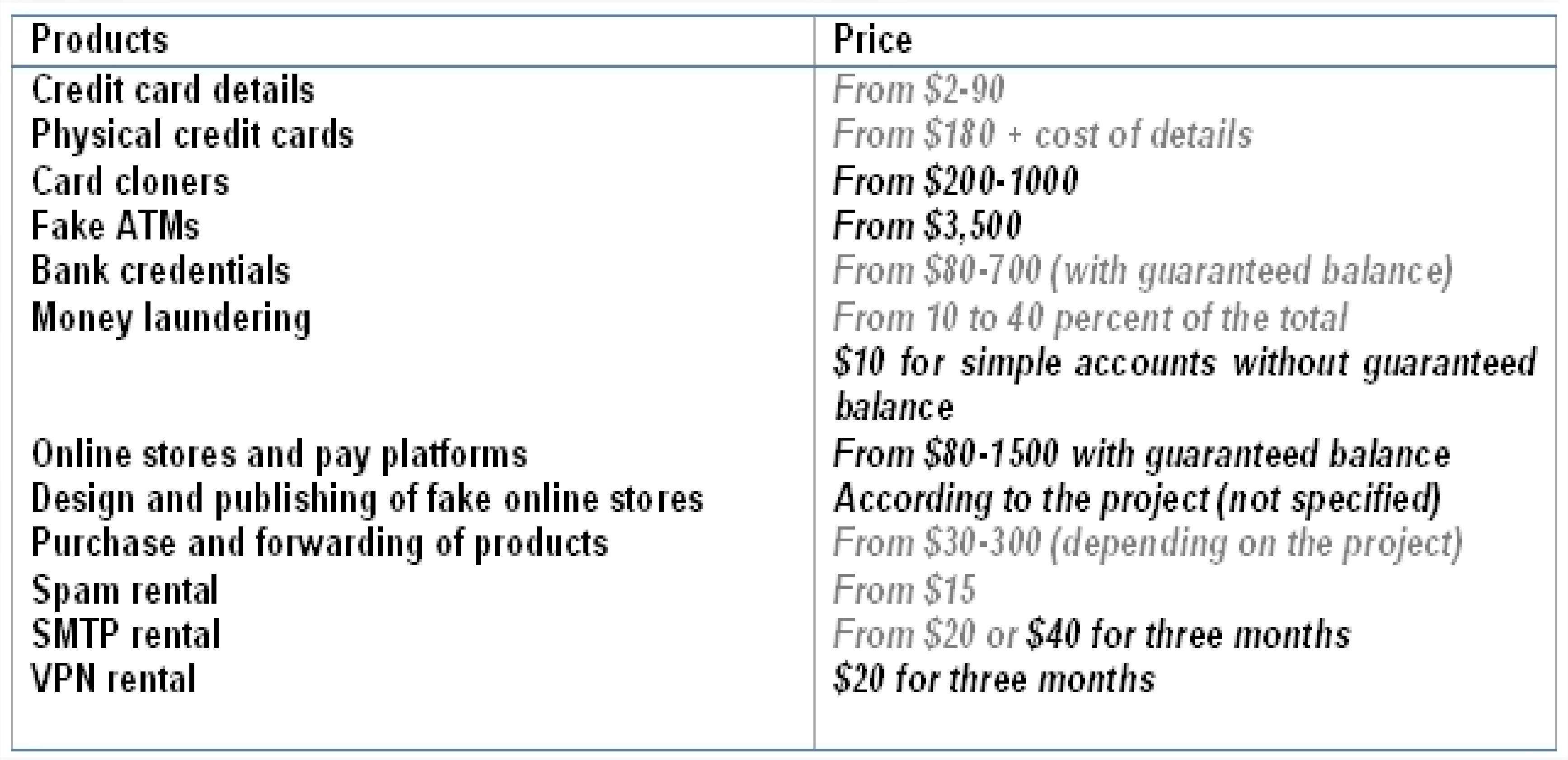
N88 | #

Accnt_[redacted]	Trans_D[redacted]	Accnt_Coc	Amount	Reference	Description

[redacted]

CostingAnalysis_[redacted]

The Cyber-Crime Black Market



Products	Price
Credit card details	*From $2-90*
Physical credit cards	*From $180 + cost of details*
Card cloners	*From $200-1000*
Fake ATMs	*From $3,500*
Bank credentials	*From $80-700 (with guaranteed balance)*
Money laundering	*From 10 to 40 percent of the total*
	$10 for simple accounts without guaranteed balance
Online stores and pay platforms	*From $80-1500 with guaranteed balance*
Design and publishing of fake online stores	*According to the project (not specified)*
Purchase and forwarding of products	*From $30-300 (depending on the project)*
Spam rental	*From $15*
SMTP rental	*From $20 or $40 for three months*
VPN rental	*$20 for three months*

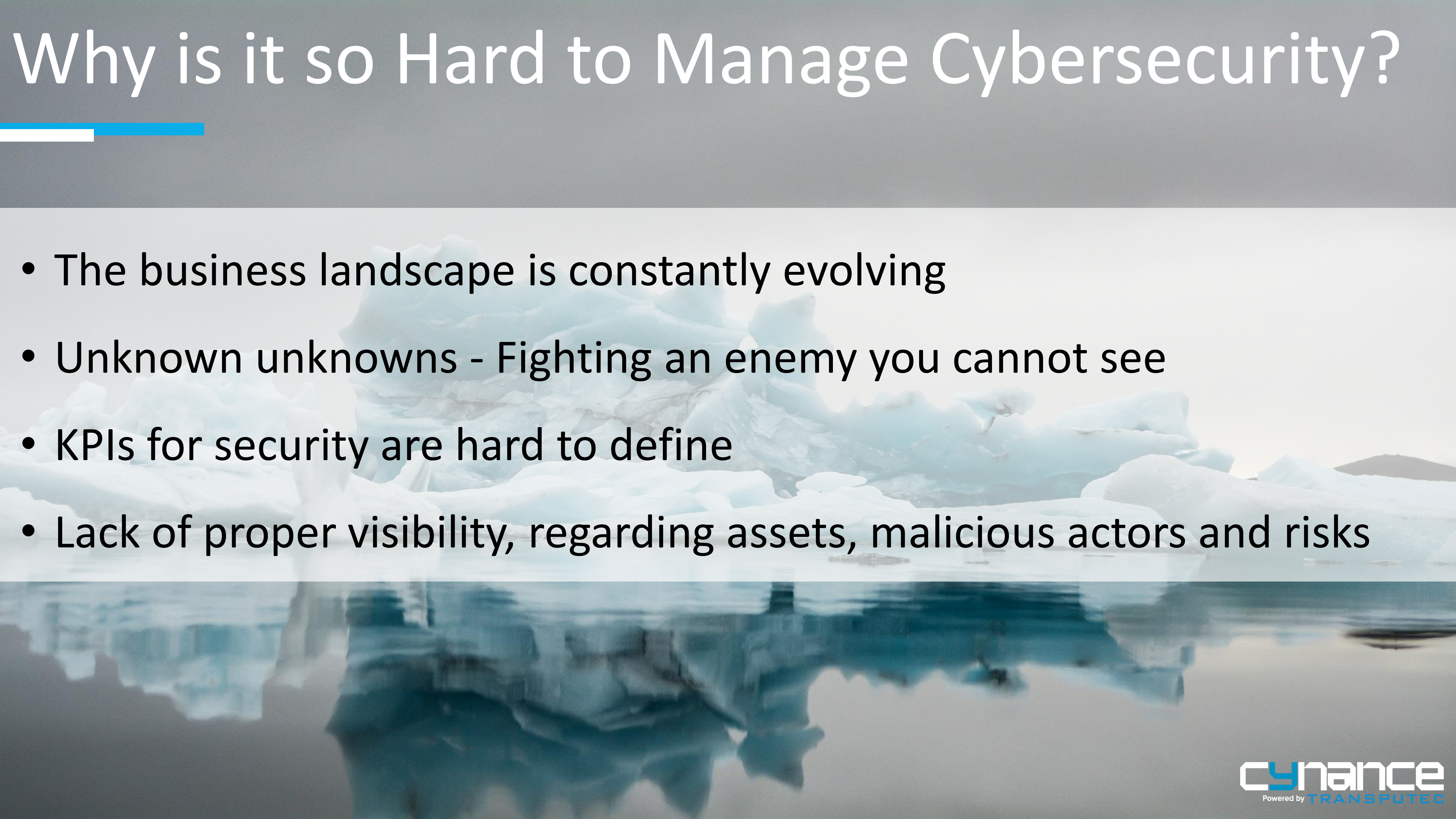
Let’s Get Practical

Why Does Your Company Need Cybersecurity?

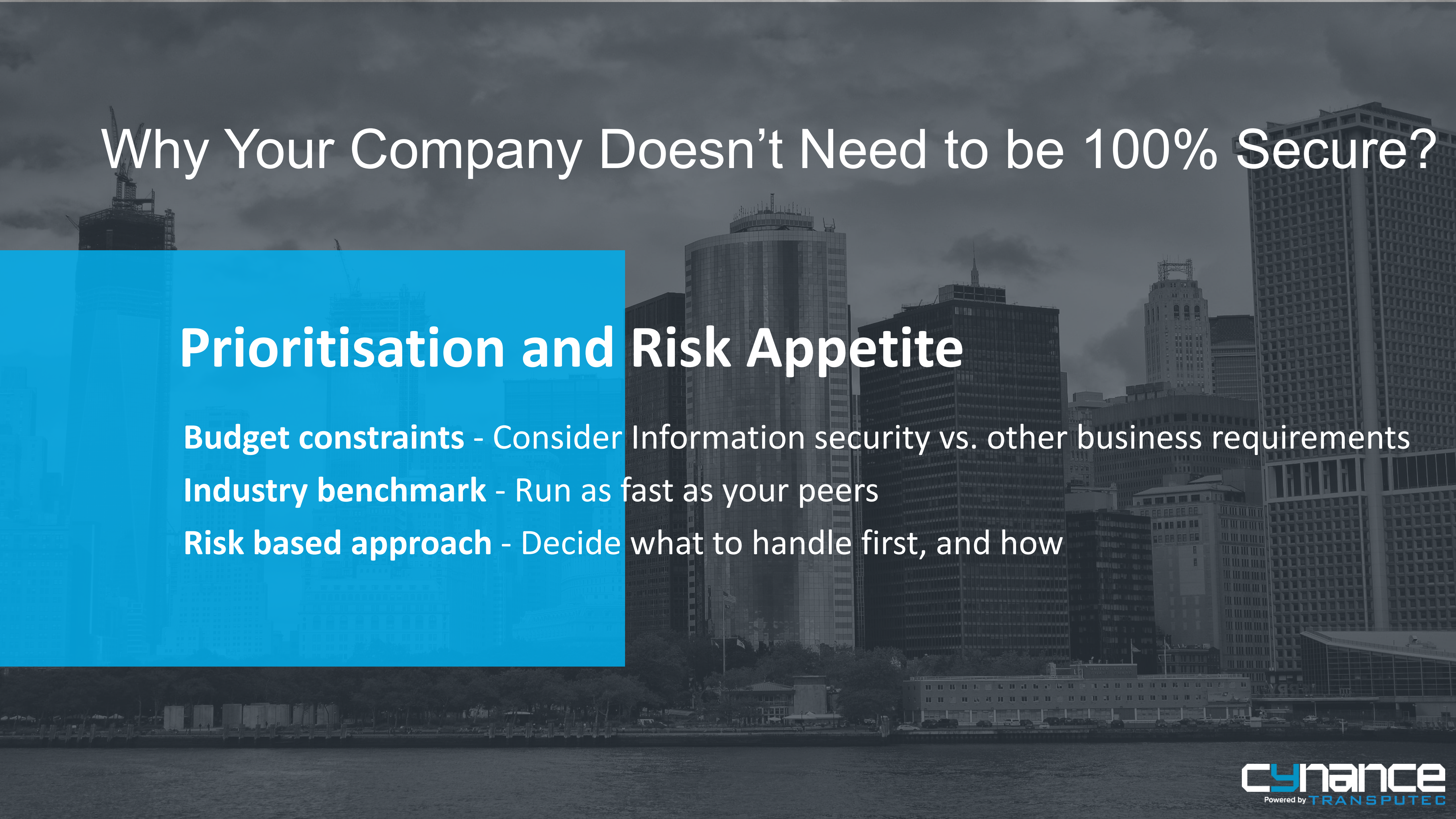
- Protect your business
- Protects your brand and reputation
- Demonstrates credibility and trust
- Provides assurance to clients that their information is secure
- Support compliance with laws and regulations
- Reduce likelihood of facing prosecution and fines
- Get a competitive advantage
- Meet customer and tender requirements
- Gain a status of a preferred supplier
- Potential cost savings through reduction in incidents
- Improves the ability to recover from adverse incidents and continue business as usual

cynance
Powered by TRANSPUTEC

Why is it so Hard to Manage Cybersecurity?



- The business landscape is constantly evolving
- Unknown unknowns - Fighting an enemy you cannot see
- KPIs for security are hard to define
- Lack of proper visibility, regarding assets, malicious actors and risks



Why Your Company Doesn’t Need to be 100% Secure?

Prioritisation and Risk Appetite

Budget constraints - Consider Information security vs. other business requirements

Industry benchmark - Run as fast as your peers

Risk based approach - Decide what to handle first, and how

cynance
Powered by TRANSPUTEC

What Are Your Crown Jewels?

Systems and Platforms

Business platforms
Critical applications
Physical and digital IT
Backups and Storage

Physical and Digital Assets

Fixed Assets
Money
Inventory
Licenses

Data Assets

IP, PII, Commercial assets, HR data

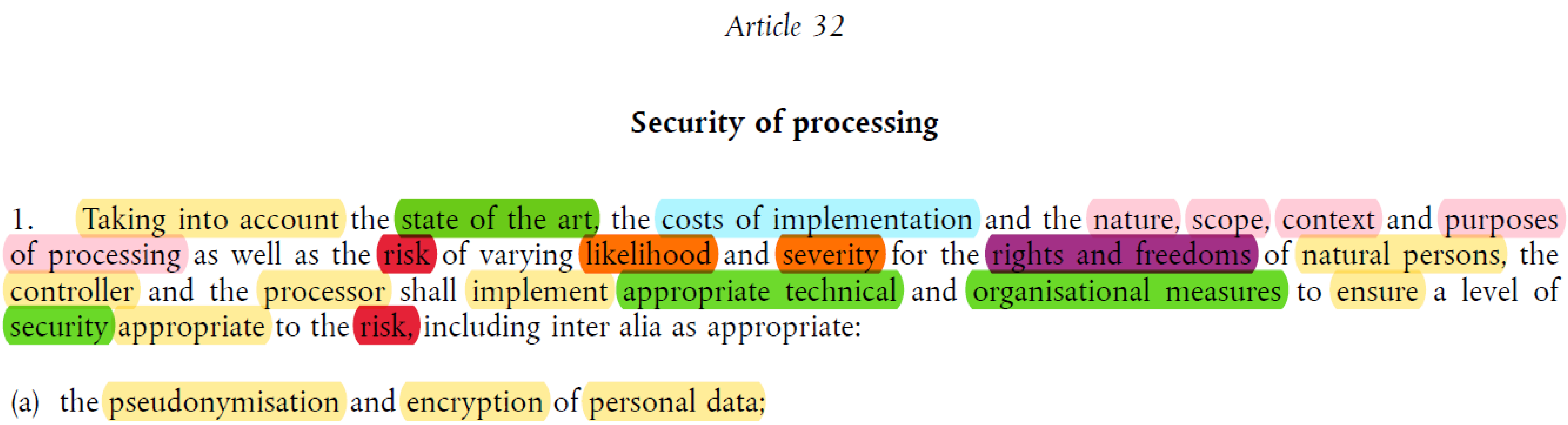
Employees Safety and Security

Environmental, Safety and security at the work place

What Are ***Your*** Cyber Threats?

- Data breach
- Insider threat
- Systems and applications weaknesses
- Insecure Application User Interfaces (APIs)
- Malware (Ransomware, Worms, Trojans, etc.)
- APT (advanced persistent threat)
- Hacking campaigns
- Phishing attacks
- Corporate espionage
- Cloud security abuse
- Shadow IT systems
- Device lost/ theft
- Intended exploitation of GDPR procedures
- DDoS (Distributed Denial of Service) Attacks

What Are your Regulatory Requirements?



Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

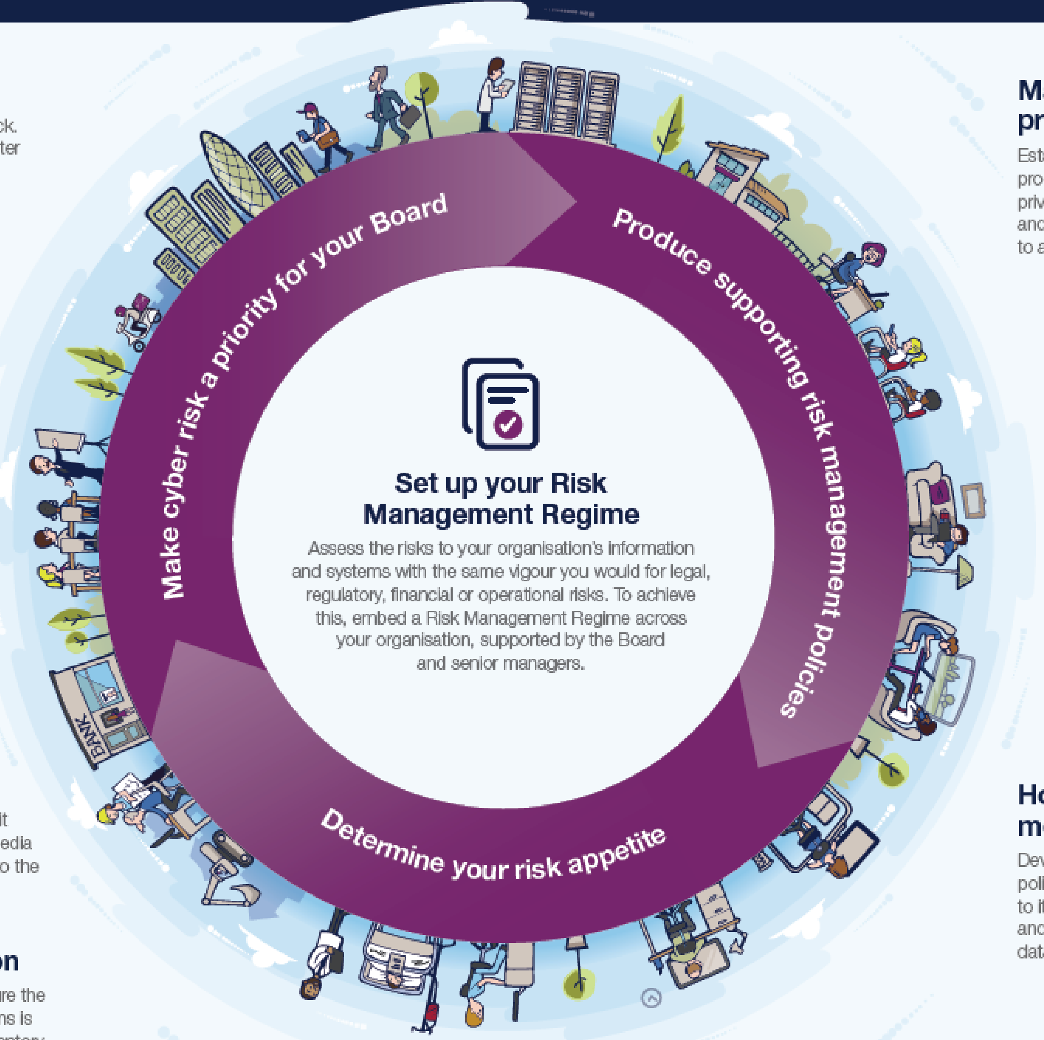
Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.



Make cyber risk a priority for your Board

Produce supporting risk management policies

Determine your risk appetite

Set up your Risk Management Regime

Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

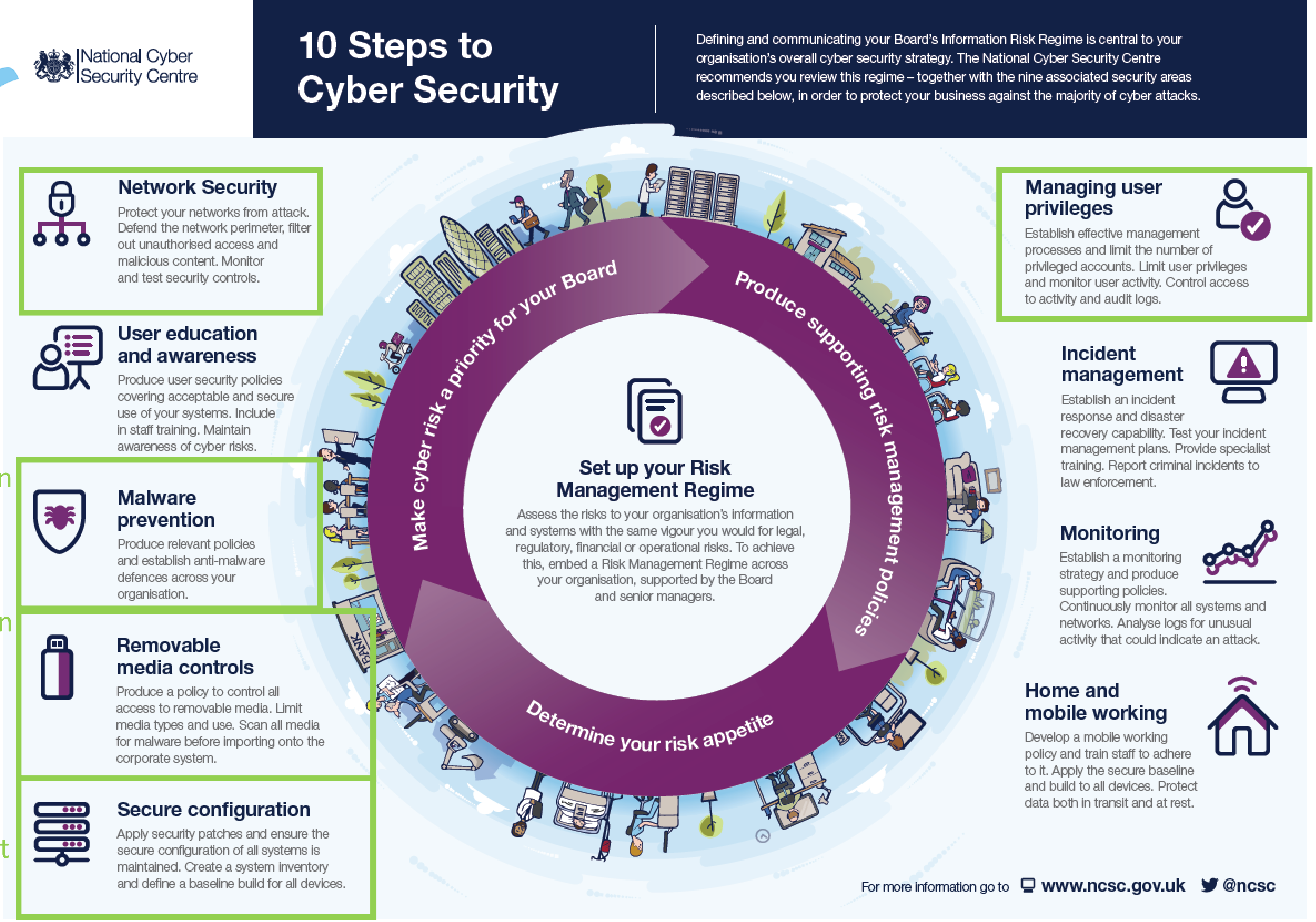
Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

CYBER ESSENTIALS

National Cyber Security Centre



10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

1. Network Security & Firewalls

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

4. Malware Protection

Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

4. Malware Protection

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

2. Secure settings

5. Patch Management

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Make cyber risk a priority for your Board
Produce supporting risk management policies
Determine your risk appetite

Set up your Risk Management Regime

Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

3. Access control

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

cynance Powered by TRANSPUTEC

CYBER ESSENTIALS

National Cyber Security Centre

ISO 27001

1. Network Security & Firewalls

A.10 Cryptography

A.13 Communications security

A.7 Human resource security

4. Malware Protection

A.12 Operations security

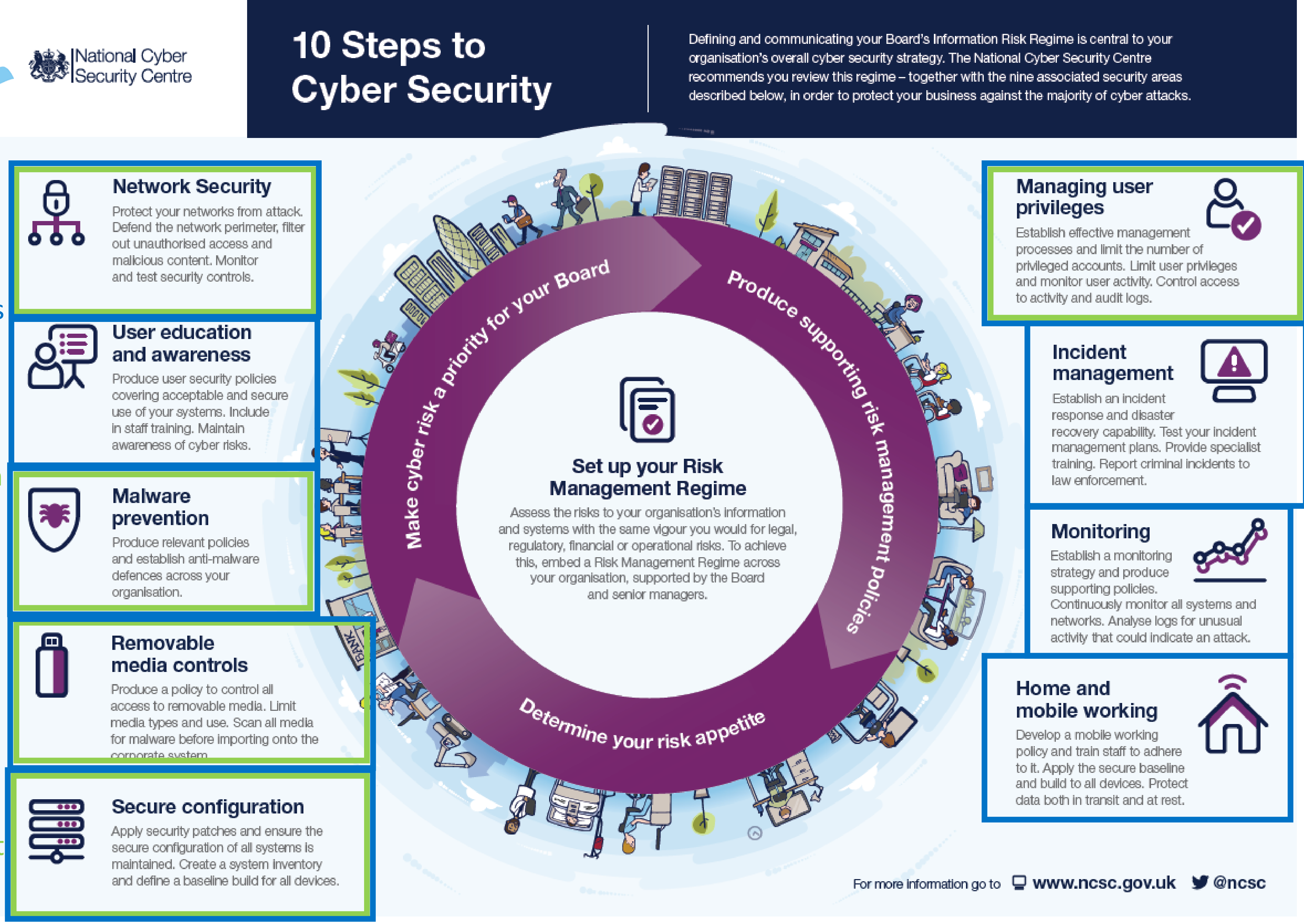
4. Malware Protection

A.8 Asset management

2. Secure settings

5. Patch Management

A.8 Asset management



10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Set up your Risk Management Regime

Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Make cyber risk a priority for your Board
Produce supporting risk management policies
Determine your risk appetite

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

3. Access control

A.9 Access control

A.16 Information security incident management

A.12 Operations security

A.6 Organization of information security

CYBER ESSENTIALS

National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

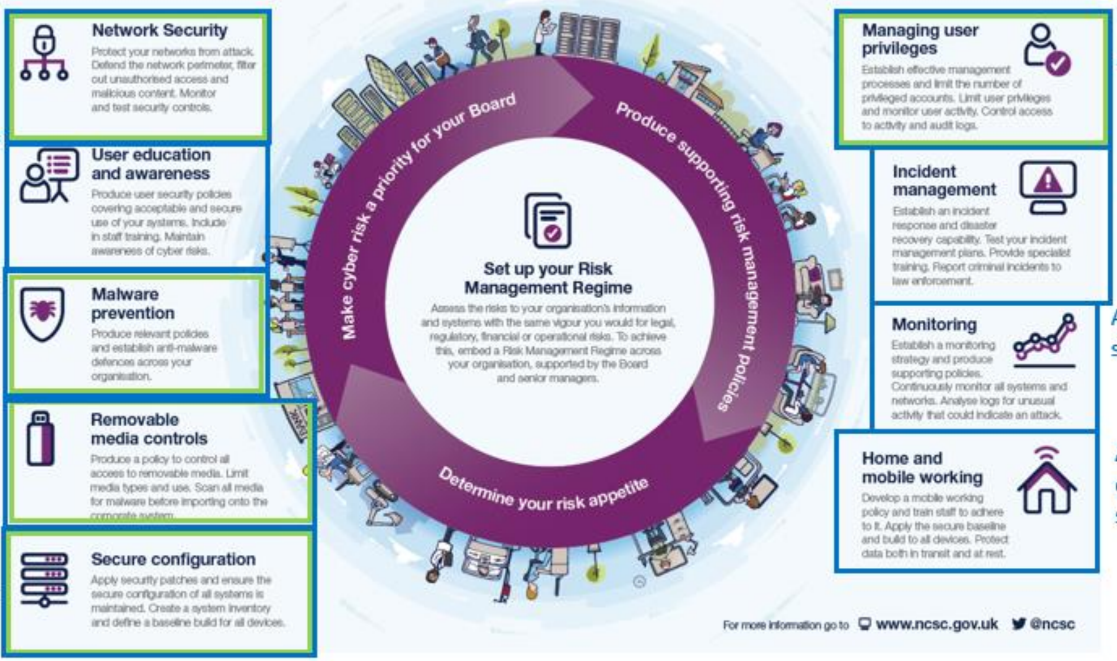
ISO 27001

1. Network Security & Firewalls
A.10 Cryptography
A.13 Communications security
A.7 Human resource security

4. Malware Protection
A.12 Operations security

4. Malware Protection
A.8 Asset management

2. Secure settings
5. Patch Management
A.8 Asset management



Make cyber risk a priority for your Board
Produce supporting risk management policies
Determine your risk appetite

Network Security
Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness
Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention
Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration
Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Set up your Risk Management Regime
Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Managing user privileges
Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management
Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring
Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

3. Access control
A.9 Access control

A.16 Information security incident management

A.12 Operations security

A.6 Organization of information security

And

A.5 Information security policies

A.11 Physical and environmental security

A.14 System acquisition, development and maintenance

A.15 Supplier relationships

A.17 Information security aspects of business continuity management

A.18 Compliance

Cybersecurity Posture Enhancement - By Cynance

OWASP Open Web Application Security Project

ISO 27001

NIST CYBERSECURITY FRAMEWORK

ico. Information Commissioner's Office

COBIT® 5 AN ISACA® FRAMEWORK

CIS Center for Internet Security®

Microsoft

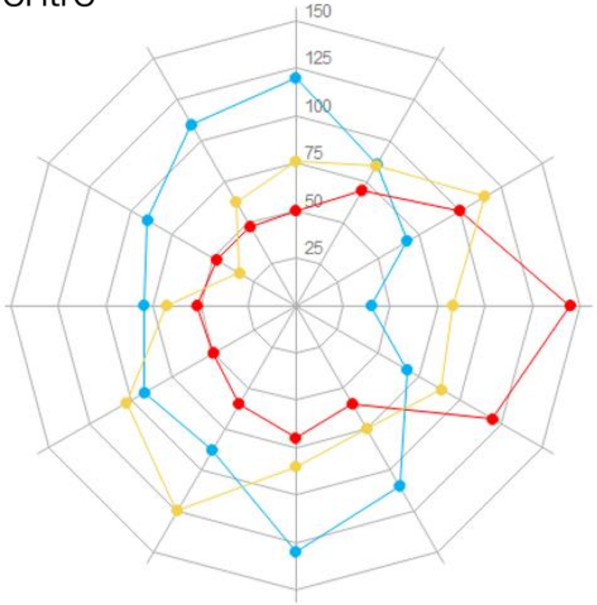
PCI Security Standards Council™

National Cyber Security Centre a part of GCHQ

SANS INSTITUTE

CSA cloud security alliance®

CREST



- 🟪 Software and Application Security
- 🟦 Network and Infrastructure
- 🟧 Secure Communication
- 🟦 Identity & Access Management
- 🟩 Threat and Vulnerability Management
- 🟨 Supply Chain Security Management
- 🟧 People Security
- 🟩 Data Protection
- 🟨 Security Governance, Risk and Compliance
- 🟥 Security Incident Response and Management
- 🟫 Business continuity management
- ⬛ Physical Security

cynance Powered by TRANSPUTEC

“

One of the main cyber-risks is to think they don’t exist. The other is trying to treat all potential risks.

”

ADJUST YOUR DEFENCE STRATEGIES

Your defence strategies have to address the security risks that are most relevant to your company

Defense in Depth

IT integration

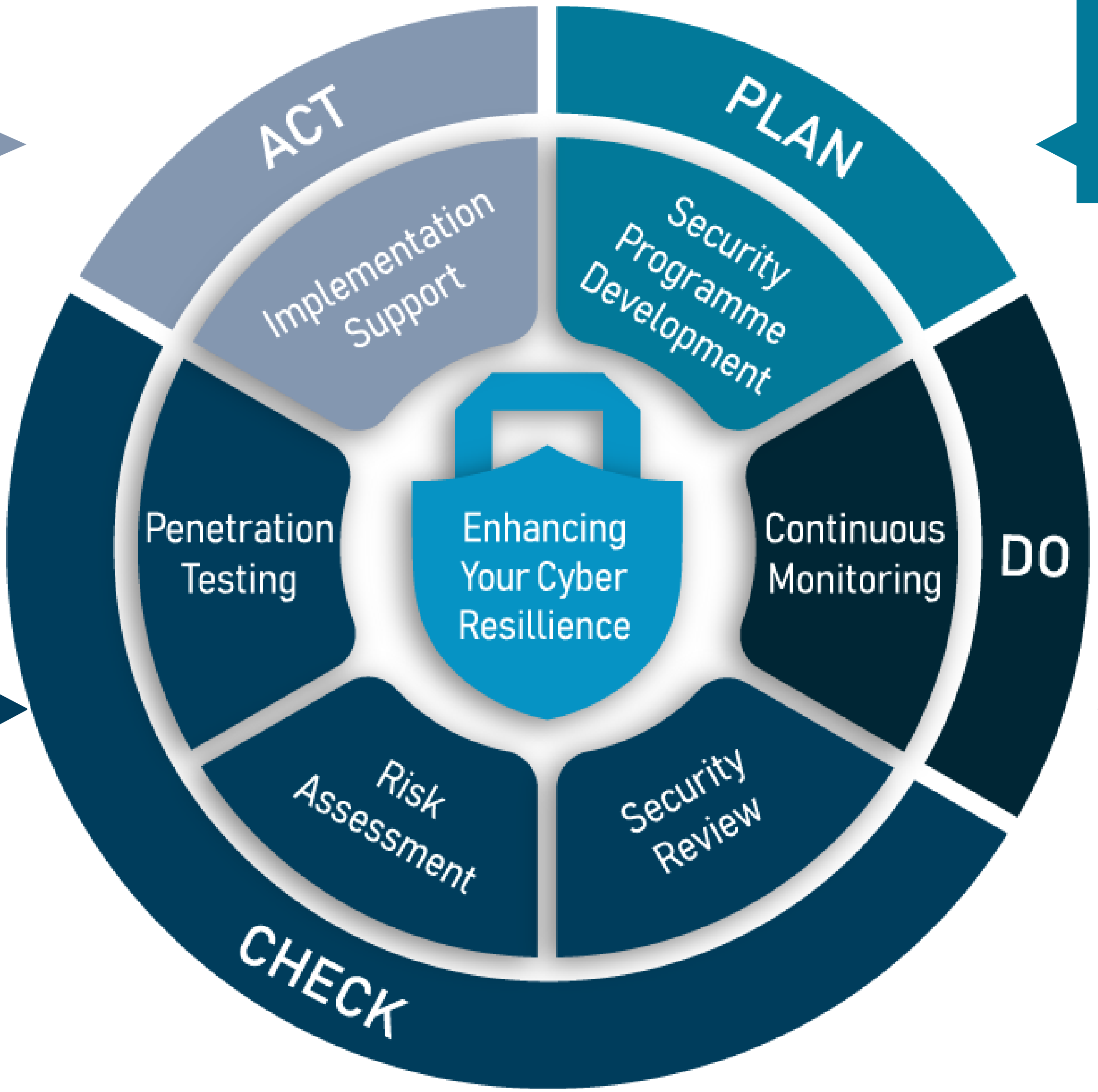
Software development

Incident Response team

Cybersecurity strategy

Security and Privacy by design

Threat Modelling



Hacking simulations

Architecture review

Security Standards Compliance

CISO/ DPO appointment

Security Operations

Threats hunting

cynance Powered by TRANSPUTEC

cynance
Powered by TRANSPUTEC

Your Cybersecurity
Business Partner

Institute
and Faculty
of Actuaries

Panel Discussion

10 February 2020

Panel discussion

Is good achievable?

How can we work better together to achieve a better outcome and how do you measure what good looks like?

Institute
and Faculty
of Actuaries

Close, network and drinks

10 February 2020