Cyber security

Digital world risk that cannot be ignored

November 2018

pwc

Who am I?

Mads N. Madsen

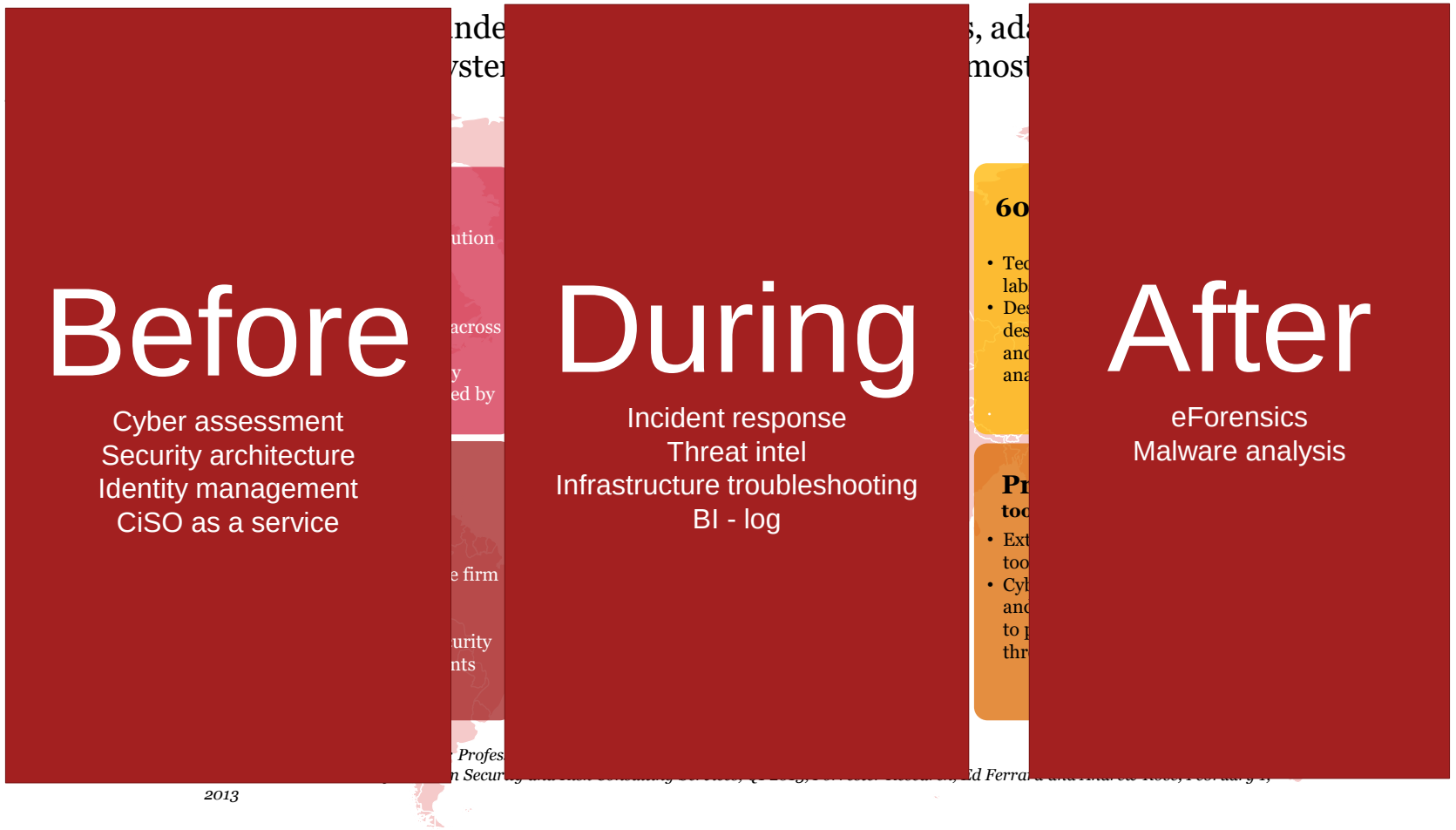
Partner – Security & Technology

Mobile: +45 2811 1592

E-mail: mads.norgaard.madsen@pwc.com

- Head of Cyber & Privacy – PwC DK
- Part of Global Cyber Leadership
- 20+ years of technology implementation experience
- Incident response adviser
- Cyber strategy through execution
- Bridging the gap between CXO and security
- Cyber strategy road map
- CXO trusted adviser

PwC – The security overview



Cyber security context

We operate in a world where we don't own the systems we use or control the data we rely on

Digital revolution

Growing cyber risk

More regulation

Cloud

"IoTs"

Digital currency

Big data

Evolving threats

More connections

Talent shortage

Arms race

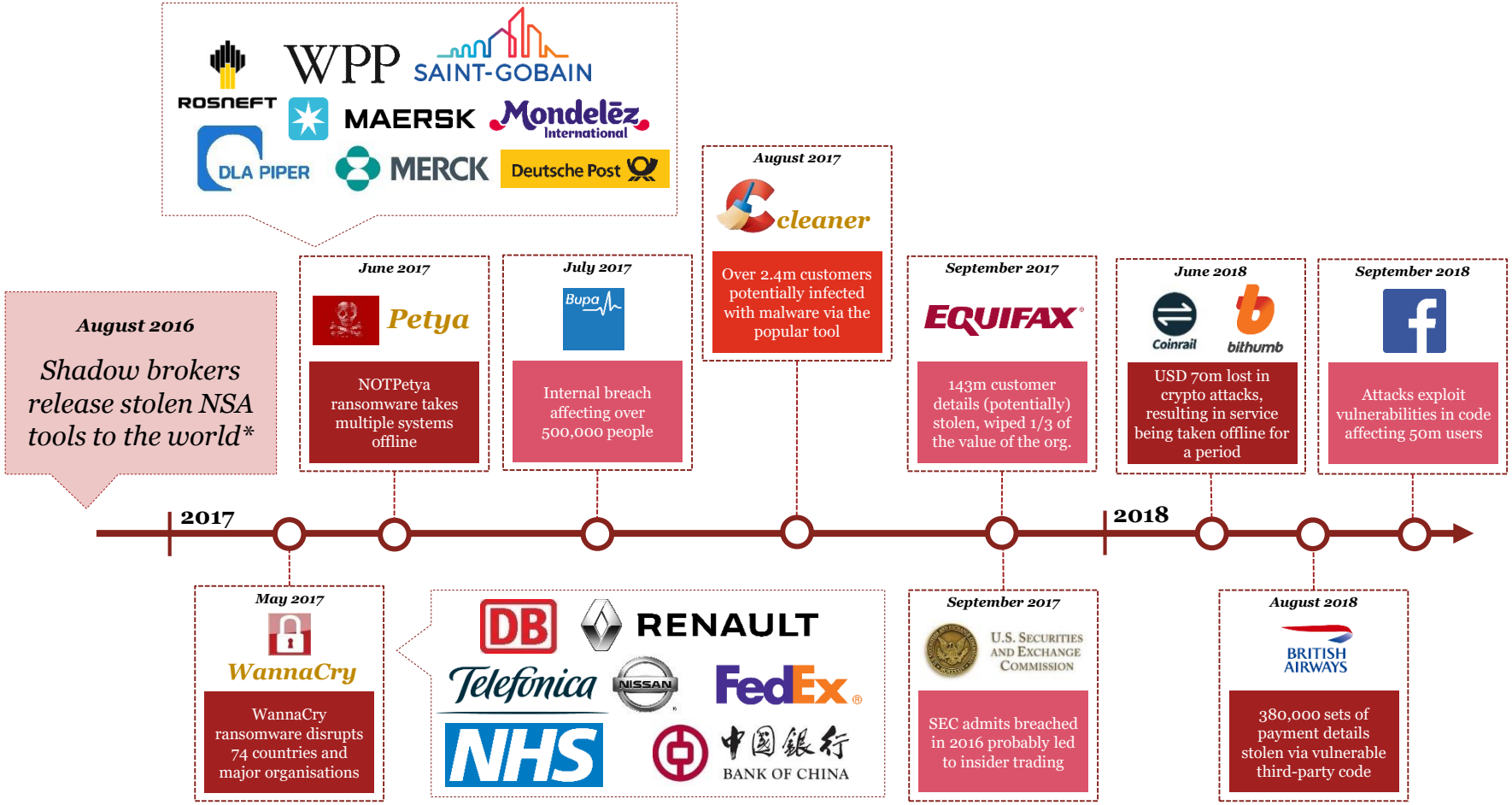
The Danish Financial Supervisory Authority

EBA EUROPEAN BANKING AUTHORITY

GDPR

Threat landscape – A lot has happened in the last 18 months …

NSA leaks have accelerated the democratisation of threats



* *The release of NSA tools has put "Nation State" tools in the hands of cyber criminals. This has resulted in a **major shift** in the **threat landscape for everyone**.*

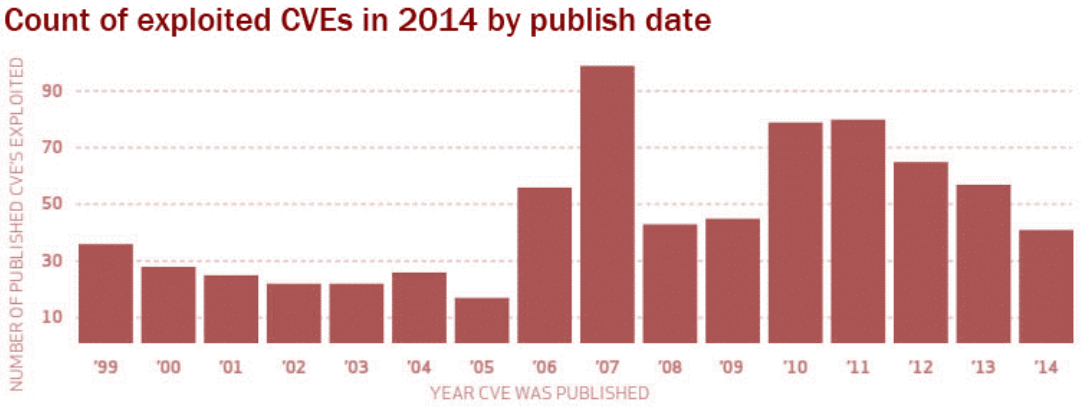
Major impacts include …

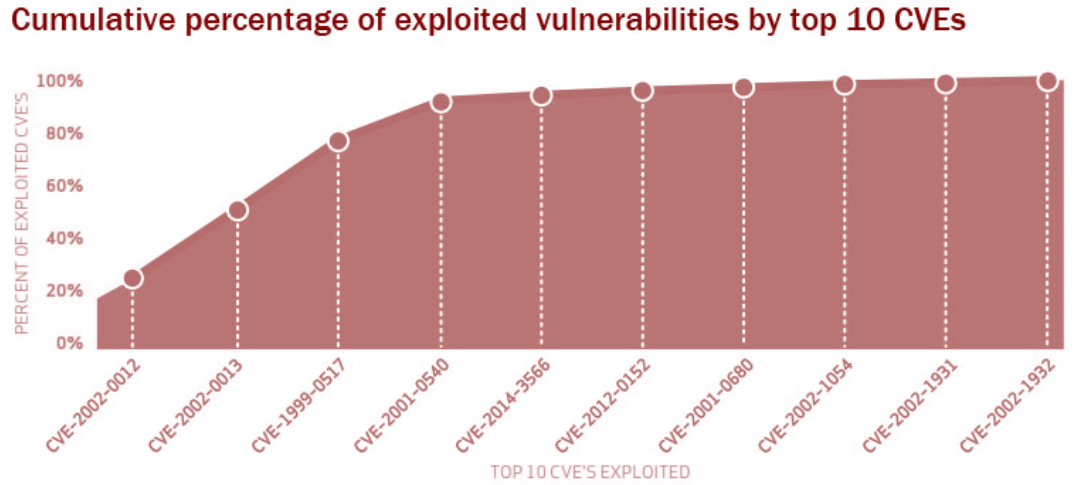
- *Maersk not being able to dock ships and unload cargo (USD 275m+)*
- *Millions of Febex (TNT) packages were delayed (USD 300m+)*
- *A global shortage of critical drugs produced by Merck (USD 300m+)*
- *Saint-Gobain had to stop major construction projects (GBP 250m+)*

Threat trend – Are we getting any better?

99.9% *of the exploited vulnerabilities (in 2014) had been identified for more than a year, some of them as far back as 1999.*

(Source: Verizon DBIR 2015)





ATM – an example of vulnerability risk

Is the RISK only ATM? What about:

Video monitoring

Cash terminals

Mobile payment

Client websites

Loyalty programs

Apps

IOT

Communication systems

Printers

Business applications

ersonal data

encrypted or
network
attack was

ound – and

l free
SB, keyboard,

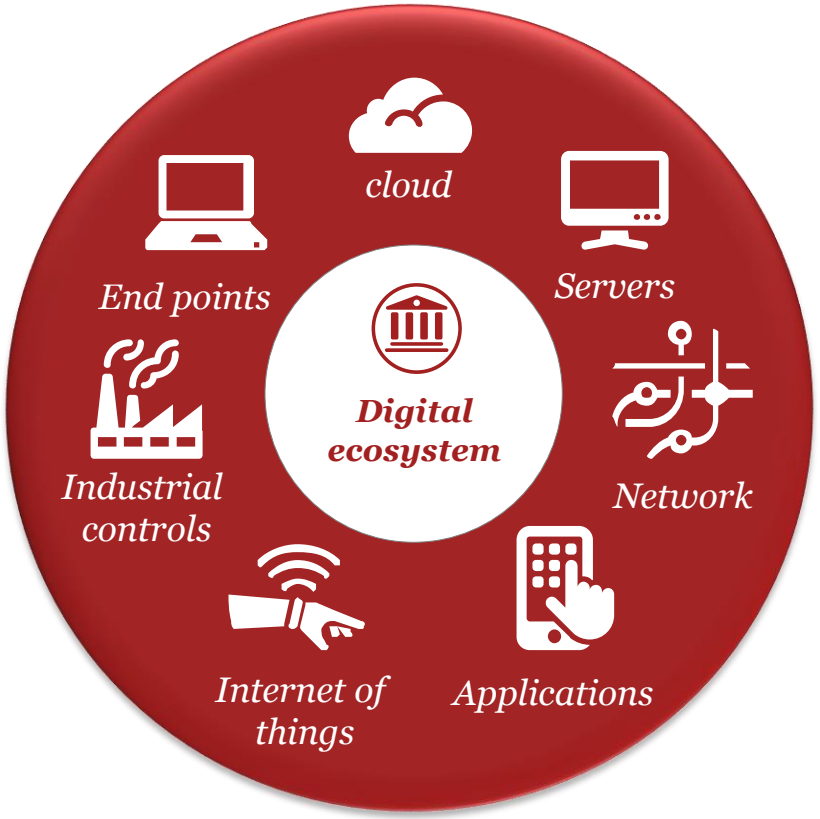
ot

vulnerable

Key reasons to protect your privileged accounts

Financial and reputational toll can be significant when compromised

1	***RISK***	***80%* of breaches involve misuse of high privileges***
2	***COMPLIANCE***	***Required to demonstrate control. (ISO 27002, GDPR, SOX, etc.)***
3	***AUDIT***	***Financial and other audits requiring you to assure control of vendor, partner and internal administrator access.***

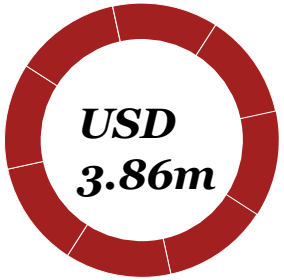


**The Forrester Wave™: Privileged Identity Management, Q3 2016*, July 8, 2016, Forrester Research, Inc.

The cost of data: Breaches within financial services

The expected loss to financial organisations from a data breach

Global average cost of a breach



6.4% increase since 2017

Predicted cost of a 'mega breach'

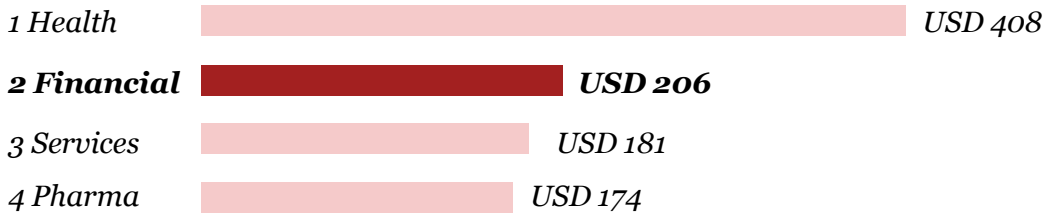
(1-50m records)

USD 40m – USD 350m

*Financial companies have the **highest number of data breaches** with the **second highest costs****

Per-capita breach cost by industry

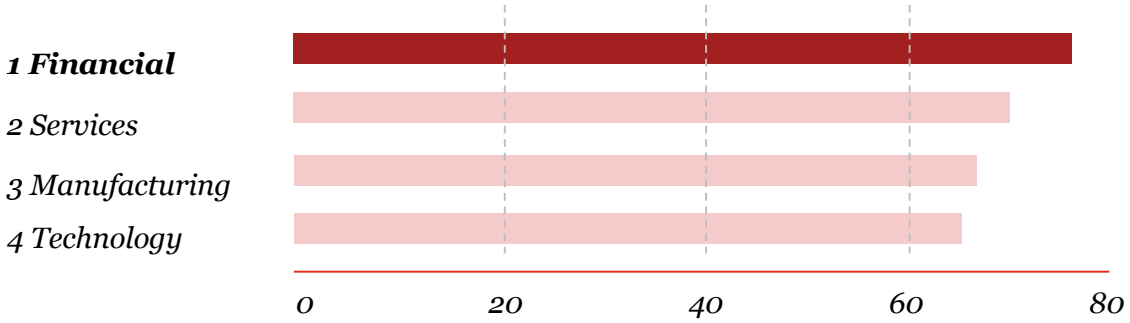
22.7% increase since 2017



Other industries include technology, energy, education and consumer to (17) public ($75 lowest per capita cost)

Frequency of data breaches by industry

27.4% increase since 2017



Based on Ponemon Institute © Research Report – 2018 Cost of Data Breach Study: Global Overview

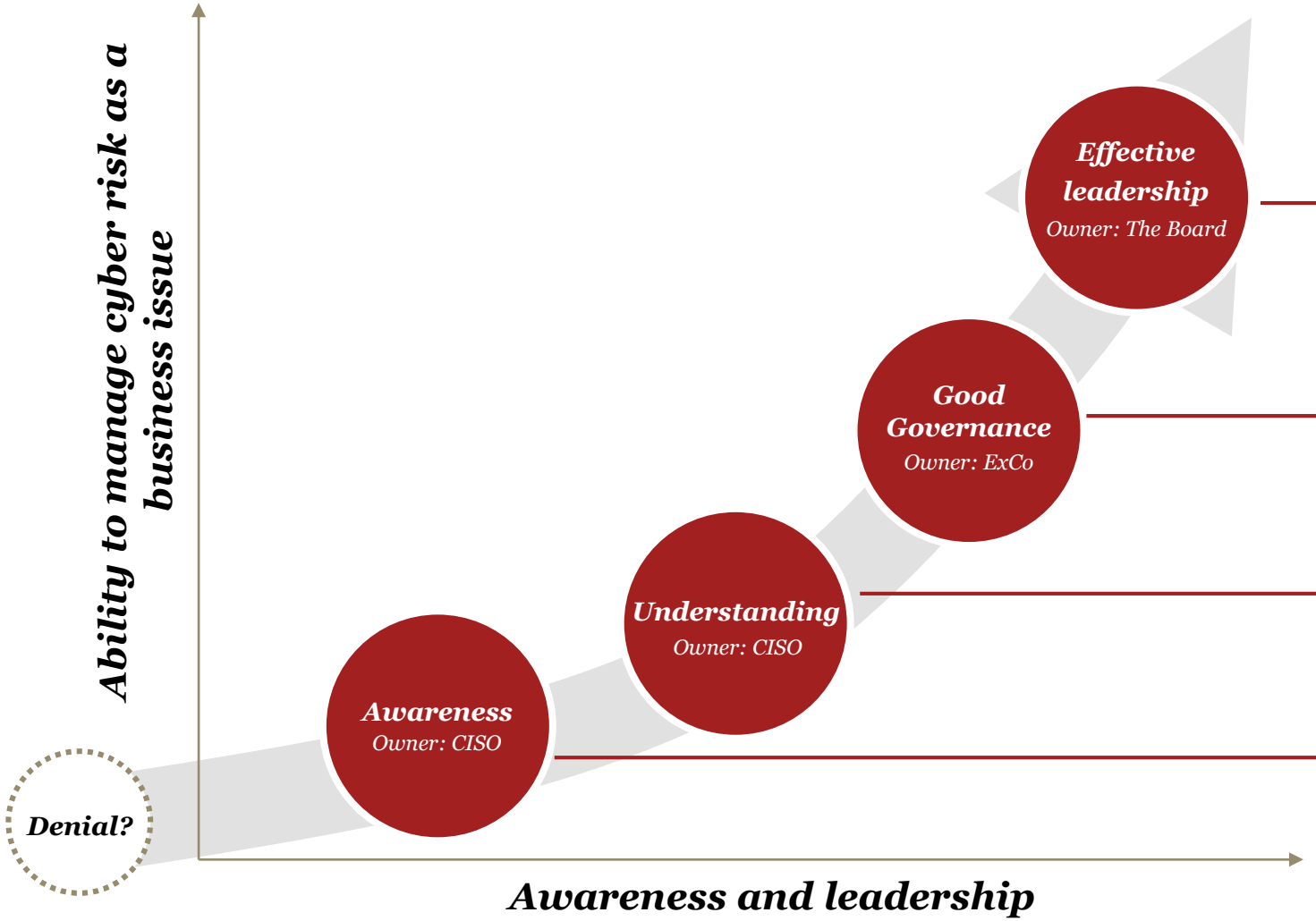
What does a typical cyber attack look like?

The majority of attacks target poor security behaviours by individuals to gain access

By understanding what real attacks look like, we can see that traditional vulnerability and penetration tests do not exercise all of an organisation's controls. **Red Team** exercises go beyond technology and look at security behaviours, detective controls and response capability to provide a more rounded and context rich view of a company's security.

Tactic/Technique			
The attacker gathers intelligence on the target organisation and its customers to refine the attack and increase the chances of success.	The attacker tricks a user to execute malicious software to compromise the user's machine or gain unauthorised access to the network.	The attacker gains more access and installs tools to monitor systems and business processes, increasing the potential impact or financial rewards for the attack.	The attacker quickly executes the attack and then removes evidence in order to prevent the target from identifying the attacker and preventing future attacks.
• Social media analysis • Digital footprint • Network scanning	• Targeted phishing emails • Social engineering	• Privilege escalation • Network traversal • Passive monitoring	• Data extraction • Financial fraud • Denial of Service (DoS)

Cyber risk management – Journey from awareness to leadership



Views from the Board

'We are leading a business in the digital age. Cyber risk is an **integral** part of innovation and growth; it is led from the top and managed by all executives'

'We actively manage cyber risk, making **well-informed choices** about how we run our business and placing clear requirements on executives. **Risk appetite influences our strategy and vice versa**'

'We maintain a well-considered cyber **risk appetite** and see **accurate management information** which demonstrates compliance'

'We understand cyber is a relevant topic and our executives **inform us** regularly'

Thank you!

Mads N. Madsen

Head of – Cyber & Privacy

Mail: mxm@pwc.dk

Cyber awareness

Modul	Indhold
1. Sikkerhed på kontoret	• Informationssikkerhed • Fysisk sikkerhed, IT sikkerhed • Medarbejderansvar • Adgangskontrol • Clean Desk • Print • Makulering

2. Beskyttelse af informationer	• Generelt om information
	  • Fortrolighed af information (Klassifikation)
	• Brug af systemer/applikationer:
	  • Installation af og brug af programmer,E-mail, Anvendelse af Cloud Services
	• Brug af enheder (pc'er, tablets, mobiler, usb
	  • IT-udstyr, Brug af egne/andres devices, Mobile enheder og USB

3. Sikkerhed på farten	• Åbne netværk • Fortrolige opkald • Fortrolige dokumenter • Devices
God adfærd på nettet	• God adfærd på nettet • Sociale medier • Streaming af film/musik • Download af filer/musik/film • Skrivning på chatboards/fora og lignende • Anstødende materiale • Sikre hjemmesider (https/kryptering)
5. Phishing	• Hvad er phishing • Phishing beskeder • IT-kriminelles perspektiv • Ransomeware • Budskaber i phishing beskederne • Avancerede phishing angreb: Spearphishing, Whaling, CEO-fraud, Vhishing, Smishing • Gode råd til at undgå at blive "fanget"

GDPR awareness

Packages		Modules
1 Processing of personal data	1	Introduction to the EU GDPR
	2	Definition of personal data
	3	Processing of personal data
	4	Lawful processing of non-sensitive personal data
	5	Lawful processing of sensitive personal data
	6	Consent
	7	General requirements regarding the rights of data subjects
	8	Information to be provided
	9	Right of access
	10	Right to rectification
	11	Right to erasure
	12	Restriction
	13	Data portability
	14	Right to object
	15	Profiling
	16	Definition of data controller and data processor
	17	Data processing agreements
	18	Supervisory authority
	19	Notification of breach of personal data security
	20	Data protection impact assessment (DPIA)
	21	Security of processing
	22	Privacy by design, and privacy by default

Game of Threats