



'Security Matters' forums are managed by Insurance Technology Forums Ltd, the specialist host of IT and security briefings for decision-makers in today's Lloyd's and London insurance market.



GDPR: why should you be interested?

Dominic Trott – Research Manager, European Security

What is GDPR?

- Replaces out of date 'directive'
- Protecting personal data (what's that?)
- Codifying rights
- Liability cannot be outsourced
- Extra-territoriality



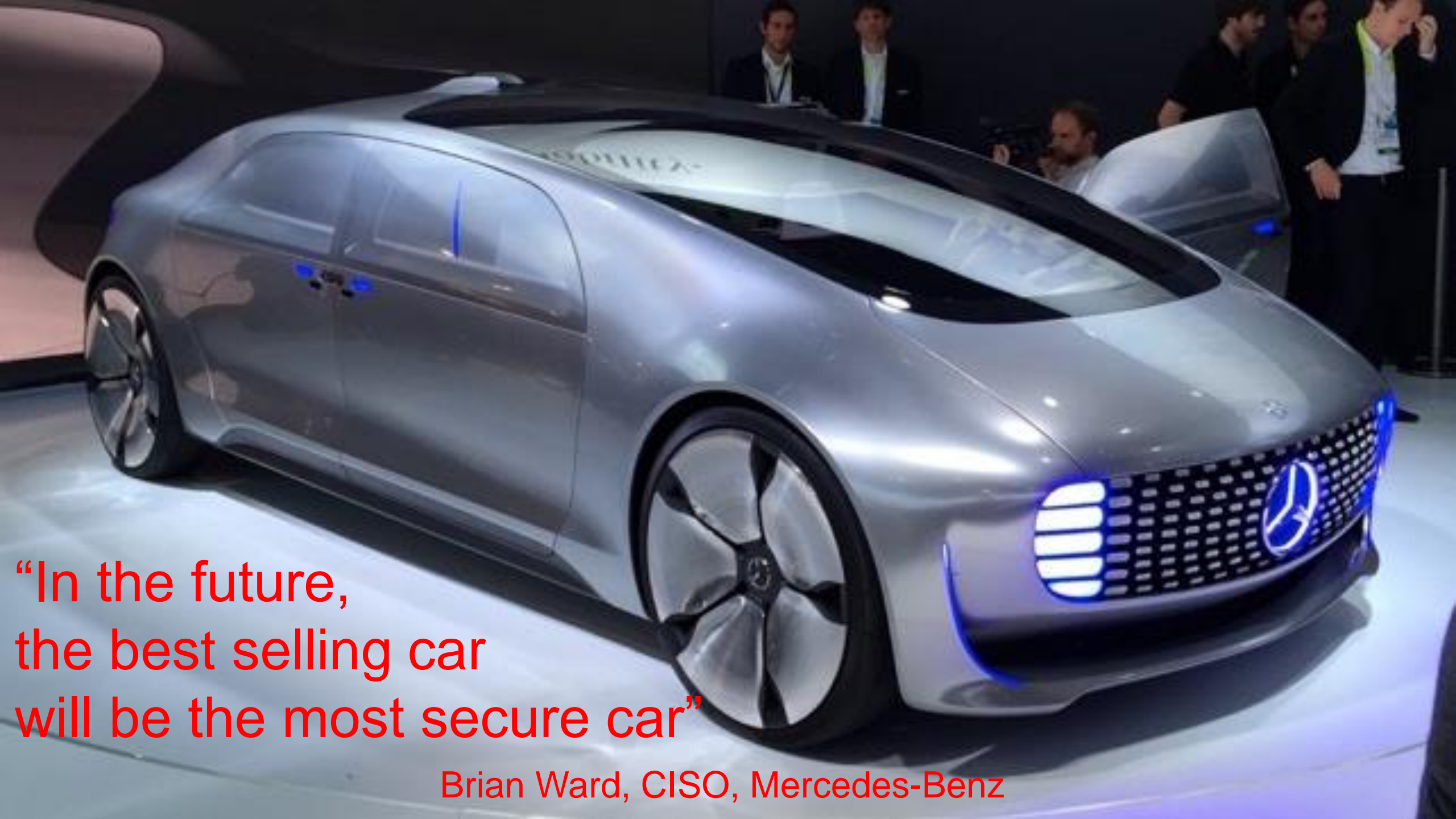
GDPR is a game-changer for enterprise risk

- Fines up to 4% of global revenues
 - “Effective, proportionate & dissuasive”
- Mandatory Breach Notifications
 - Risk to brand reputation
- Ban on personal data processing
 - In extreme cases
 - See article 58 (powers of supervisory authorities)
- Class action lawsuits
 - Right to be collectively represented (by not-for-profit bodies)
 - See article 76 and Recital 112



Is it all doom and gloom?





“In the future,
the best selling car
will be the most secure car”

Brian Ward, CISO, Mercedes-Benz

GDPR talks about ...

“State of
the art”



Cost



Risk



Context



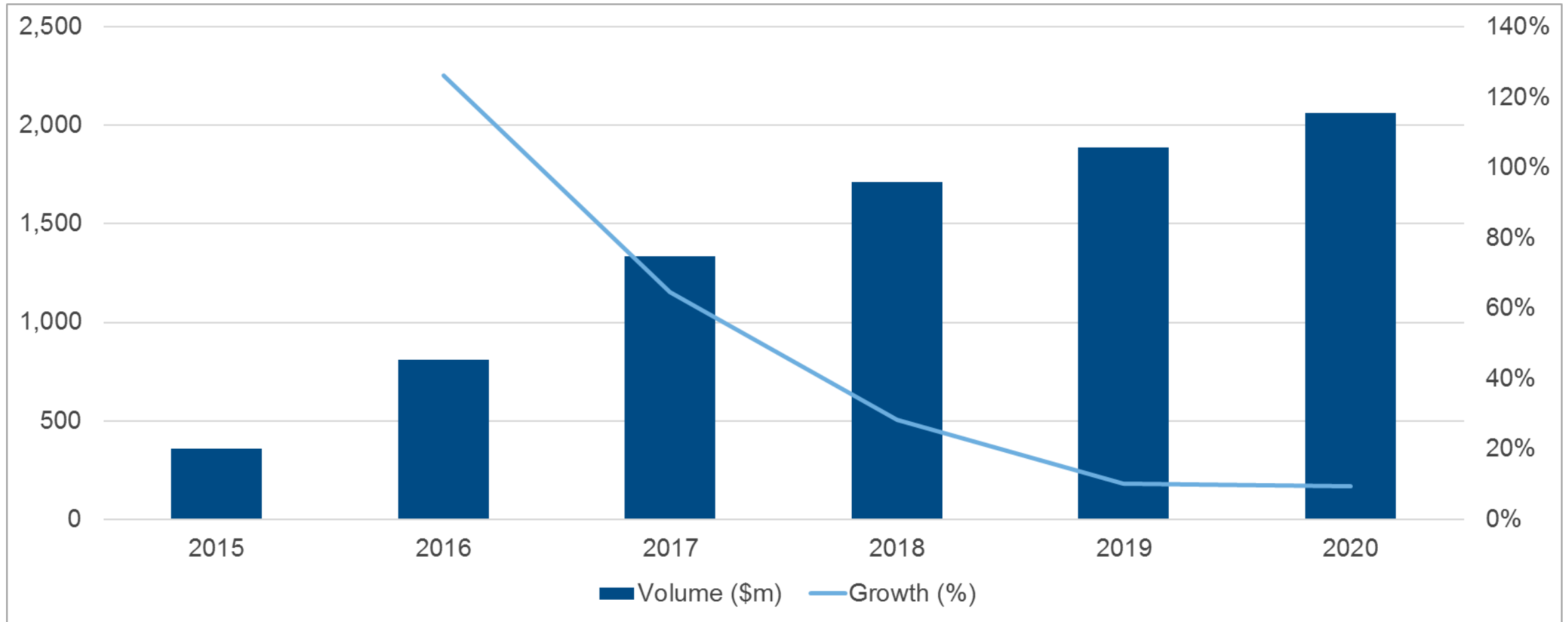
Grasp the GDPR Opportunity!



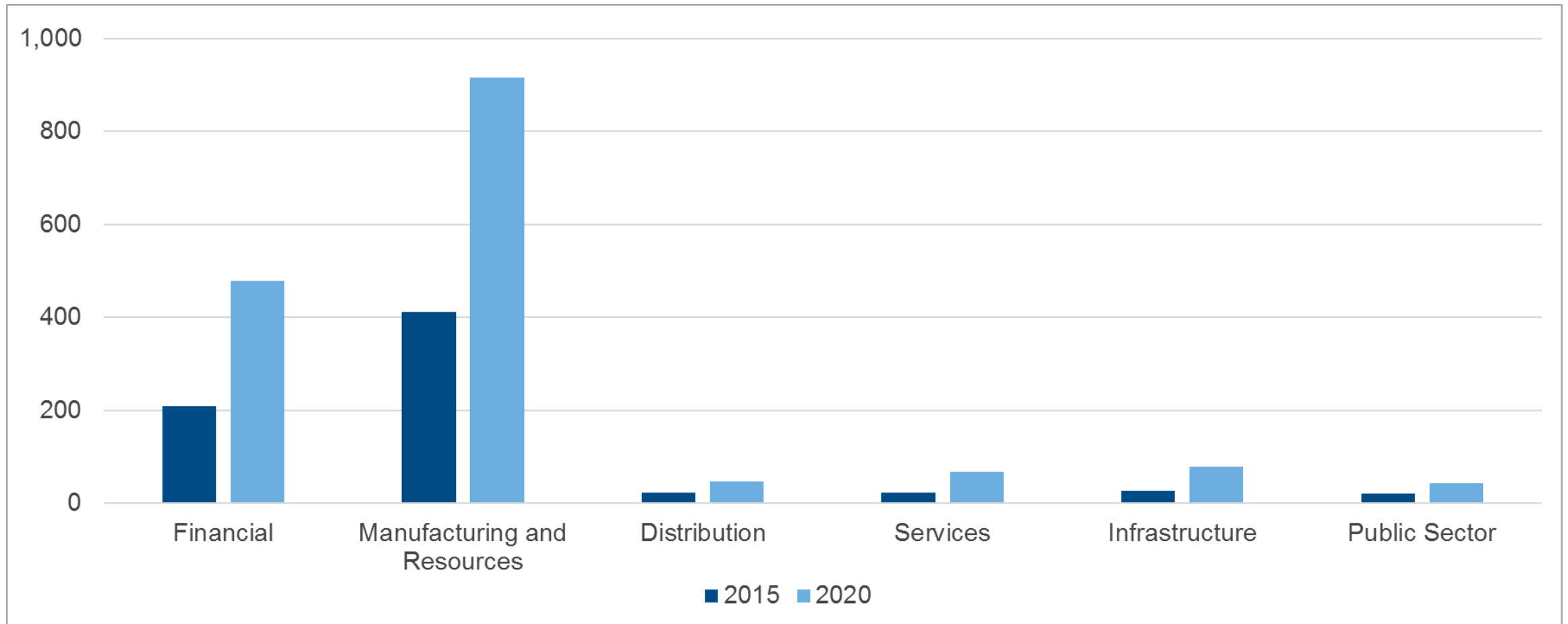
Data lifecycle – a foundational tool



Western Europe GDPR Security SW Forecast



WE GDPR Security SW Forecast by Verticals



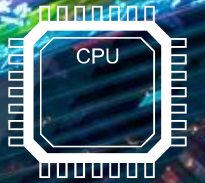


GDPR - Threat or Opportunity?

Paul Tempest-Mitchell, DELL EMC



**Constant exponent
every 5 years**



Pivotal™

SecureWorks®

RSA®

DELL

virtustream

Technologies

“Number 1 in Everything...All in One Place”

DELLEMC

vmware®

We know that the vast majority of accidents are caused by human error



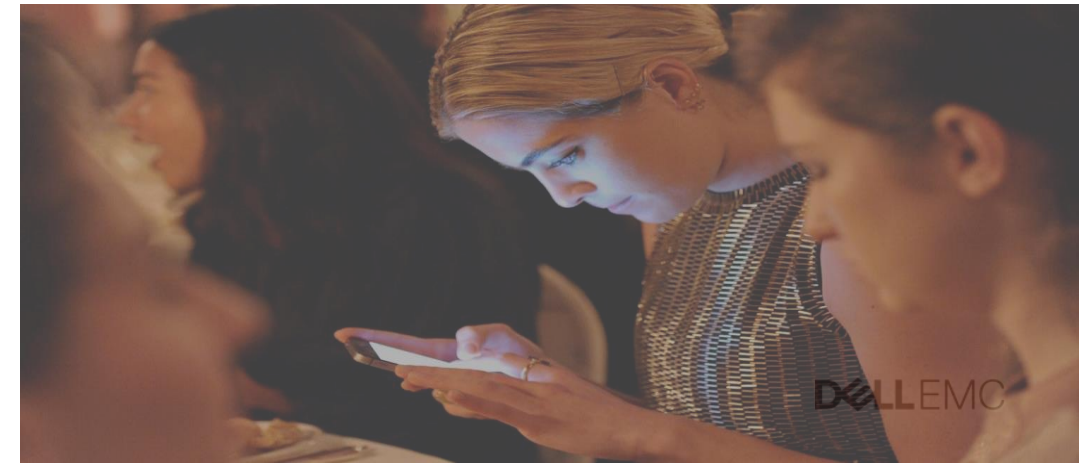
Big Data and Predictive Analytics to predict which truck drivers will have an accident



Big Data based Fraud detection can work in Real-Time



Big data could lower rates for optimistic tweeters



Opportunity: Build a Data Lake for Digital Transformation AND GDPR

DATA DRIVEN PRODUCTS & SERVICES

NEW REVENUE, COMPETITIVE EDGE, LOYALTY

FRAUD & COMPLIANCE ANALYTICS

ANTICIPATE, PREVENT, COMPLY

CUSTOMER ANALYTICS

360 VIEW OF THE CUSTOMER

REGULATORY ANALYTICS

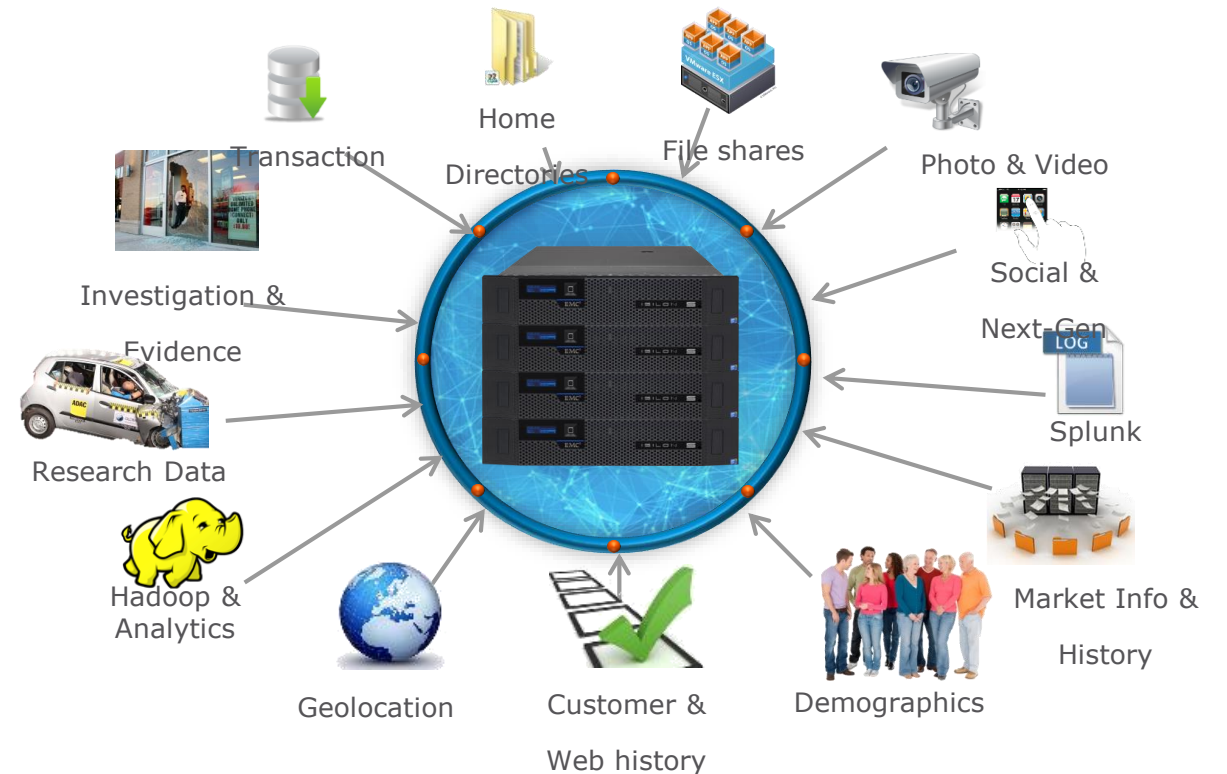
RIGHT OF ACCESS, SECURITY

OPERATIONAL ANALYTICS

ANALYSE, PREDICT, OPTIMISE

ISILON – Data Consolidation

- Secure Data in one place
- Simplify Management & Operational Costs
- Establish Data Governance and Control
- Searchable Data Lake



Is all your GDPR Data in the Data Centre?



Legacy Applications



Mobile & BYOD



Tapes



Legacy Infrastructure



Branch Office



Off-Site Tapes

Opportunity: Archive and Backup

Don't keep too much data too long.

- Copies of data are proliferating in companies – Average companies hold 19 copies of data
 - SNAPS, 7 x Day Backups, Weekly Backup, Monthly Backup.....
- Archive Data that doesn't change onto Cheap on-line storage
 - On-line = accessible and reliable and with acceptable latency for your applications
- Centralise your Backups
 - Remote/Branch office Tapes will be a GDPR problem!
- Backup to De-Duplicated Disk
 - Shorter restore windows
 - One copy of data (Dedupe) reduces legal argument for access



Data Domain Disk Based Copy Protection

Can you prove you're compliant?



Opportunity: e-Governance, Reporting and Compliance

- Automate your reporting procedure
- Consolidate regulatory requirements/process
- Consistent Approach single
- Simple operation/action



GDPR is an Opportunity

A Data Lake builds Business and GDPR Control

Take control of Copy Data and Archive – remove Tape!

Automate Governance and Reporting





RECIPROCAL

Secure Data Analysis

Dave Knock

dave.knock@reciprocalgroup.co.uk

Steve Withers

stephen.withers@reciprocalgroup.co.uk



www.reciprocalgroup.co.uk

DELL EMC

Reciprocal – Fresh GDPR Insight



Value-added Solution Provider

**Consult, Design and Implement
complex IT Solutions**

**Specialists in Data Management and
Migration Services**

105% growth 2016

100% Customer satisfaction



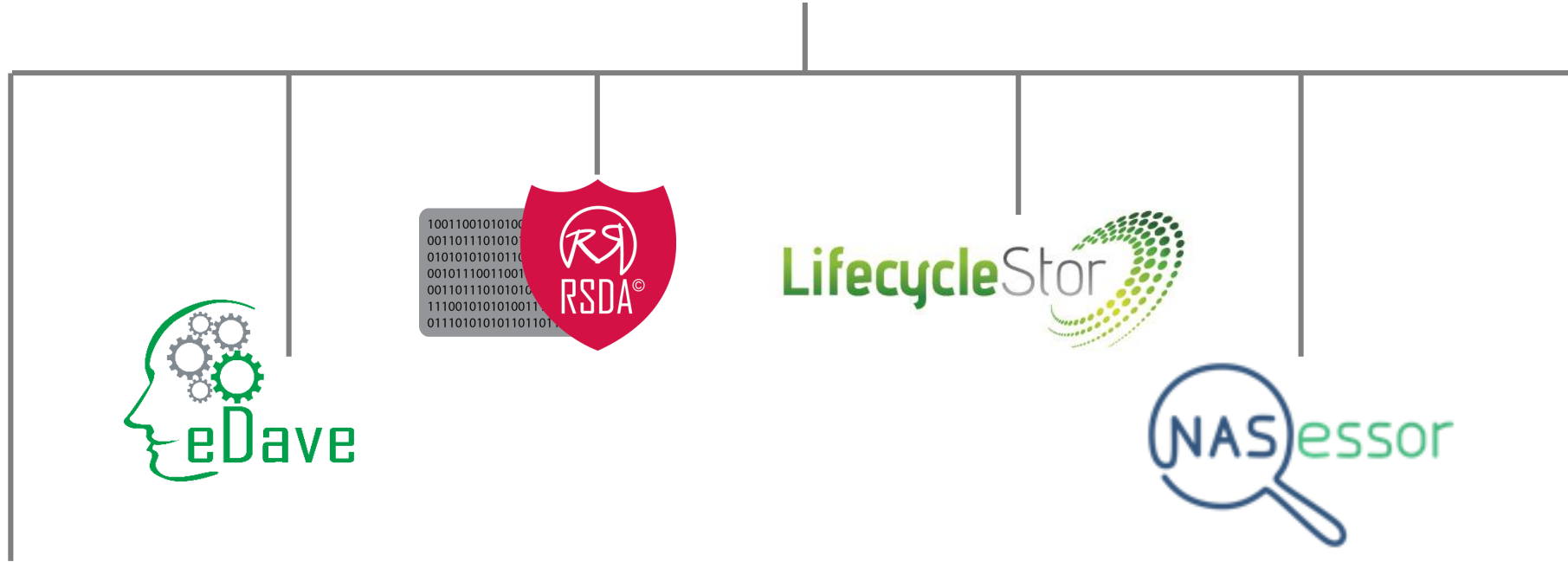
www.reciprocalgroup.co.uk

DELL EMC



RECIPROCAL

embracing technology & innovation



10011001010100
0011011101010
01010101010110
00101110011001
00110111010101
11100101010011
0111010101011011



RECIPROCAL
Global Consulting
Services

Data Migration Specialists

RECIPROCAL
Managed Services



www.reciprocalgroup.co.uk



GDPR

Where do you start?

What is your plan?



GDPR
approaching



Context



Advantage



Impact



Automate



GDPR Background

GDPR sweeps away the Data Protection Act of 1998



New Philosophy

- People have a right to Protection & Control of their personal data
- Companies/holders of data are now held responsible for the protection of Personally Identifiable Information (PII)
- Any data subject has the right to access their PII data



GDPR
approaching



Context



Advantage



Impact



Automate

How ready are you?

Food for thought - *DELL GDPR Global Survey 2016 (850 respondents)*

79% of respondents currently say they would not, or were not aware whether their organisation would face penalties in its approach to data privacy IF GDPR had been in effect this past year.

Of the remaining **21%**...



36%

don't know the penalties

50%

Believe they would face moderate fines

25%

expect significant IT changes

90%

said their existing practises will not suffice



**GDPR
approaching**



Context



Advantage



Impact



Automate

Impact

Business Impact

Procedures, people and policy



IT Impact

Vulnerability landscape,
data management and security



GDPR
approaching

- ☐ Context
- ☐ Advantage
- ☒ Impact
- ☐ Automate

Impact - Business

Procedure, people and policy

Raise awareness – *communicate with Executive decision makers*

Review and update privacy notices – *what data, how is it shared?*

Have a legal basis to process personal data – *Why is PII collected?*

Review consent – *should be freely given, specific informed, unambiguous*

Look after children – *how will age be verified?*

Procedure for data breaches – *communicate to ICO*

Appoint a DPO – *Consider outsourcing. Take it seriously*



GDPR
approaching

- ☐ Context
- ☐ Advantage
- ☒ Impact
- ☐ Automate

Sources – IDC GDPR Exec brief 2016, Iron Mountain Practical Guidance, Accenture GDPR overview

Impact – IT

Vulnerability landscape, data management and security

Locate information – Document PII data held, what, where how stored.
Undertake an information audit inside and outside organisation

Know Individuals' rights – the right of access, the right to rectification
and the right to erasure

Be ready for subject access requests – from 40 days down to 1 month.
Beware potential class actions



GDPR
approaching



Context



Advantage

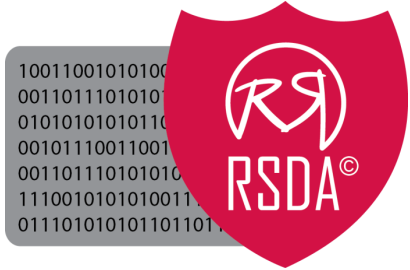


Impact



Automate

Automate Discovery



Solution Suite

- Collaborative Consultancy
- DC Audit and review
- NASessor file system analysis
- Automated PII data sniffing
- Data access assessment
- Automated data transfer and deletion



GDPR
approaching



Context



Advantage



Impact



Automate



On average, each employee stores **10GB** of unstructured data

1%

of documents contain passwords

9%

contain personally-identifying information

42%

are company sensitive

46%

is duplicated information





Personal data could be anywhere





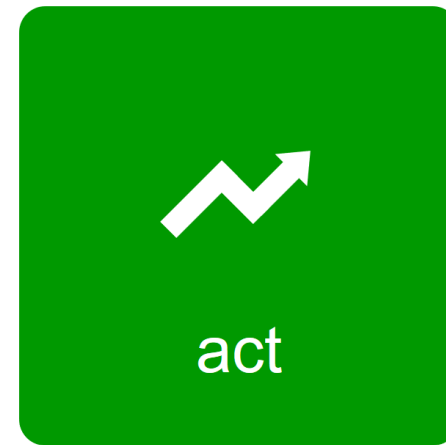
You need to know where it is



www.reciprocalgroup.co.uk



Information Intelligence; the key to unlocking your data



[illegible]



Searches Duplication Alerts Exports Reports Settings Help

Logged in as dave.knock | Log out

ACTIONS

DATA SETS

Data Sets Searched ☒ All

- ☒ Uncategorised
- ☒ Wikileaks
- ☒ Airships
- ☒ Cryptome
- ☒ Sonyhack

COLUMNS

Show columns by:

- ☐ Author
- ☐ Company
- ☒ Content Type
- ☐ File Type
- ☐ Tags
- ☐ Show All Results As One Column

Data Set: Sonyhack
ContentType: application/multipart
Count: 133,151

Total Documents | File Size: **290,544**

RECIPROCAL





Searches Duplication Alerts Exports Reports Settings Help

Logged in as dave.knock | Log out

RECIPROCAL

ACTIONS

DATA SETS

Data Sets Searched ☒ All

- ☒ Uncategorized
- ☒ Wikileaks
- ☒ Airships
- ☒ Cyptome
- ☒ Sonyhack

COLUMNS

Show columns by:

- ☐ Author
- ☐ Company
- ☒ Content Type
- ☐ File Type
- ☐ Tags
- ☐ Show All Results As One Column

Query Simple Search X

Drag a field over to start your query

+ Body Match Words Mastercard Visa X

AND

+ CreditCardCount is from 10 to X

Common

File System

Multimedia

Personal Information

- Credit Card Count
- Credit Cards
- Email Address Count
- Email Addresses
- NI Number Count
- NI Numbers
- Postcode Count
- Postcodes
- Telephone Number Count
- Telephone Numbers

Other

Pre-Loaded Queries

Clear Refresh Refresh & Close

Total Documents | File Size

290,544

Icons: [Thumbnail] [Thumbnail] [Thumbnail]





Searches

Duplication

Alerts

Exports

Reports

Settings

Help

Logged in as dave.knock | Log out

RECIPROCAL

ACTIONS

DATA SETS

COLUMNS

CURRENT QUERY

Data Sets Searched

☒ All

☒ Uncategorized

☒ Wikileaks

☒ Airships

☒ Cryptome

☒ Sonyhack

Show columns by:

☐ Author

☐ Company

☒ Content Type

☐ File Type

☐ Tags

☐ Show All Results As One Column

Body ?= "Mastercard Visa"

AND

CreditCardCount FROM "10" TO ""

Total

Documents | File Size

15

Data Set: Uncategorized

ContentType: application/ms-excel

Count: 3

W

100%

100%





SearchesDuplicationAlertsExportsReportsSettingsHelp

Logged in as dave.knock | Log out

ACTIONS

DATA SETS

Data Sets Searched

☒ All

☒ Uncategorized

☒ Wikileaks

☒ Airships

☒ Cryptome

☒ Sonyhack

COLUMNS

Show columns by:

☐ Author

☐ Company

☒ Content Type

☐ File Type

☐ Tags

☐ Show All Results As One Column

CURRENT QUERY

Body ?= "Mastercard Visa"

AND

CreditCardCount FROM "10" TO ""

Document Results: 3

page 1 of 1

	ApplicationName	FileName	Tags
<input type="checkbox"/>	Microsoft Excel	Deskinfo..xls	-
<input type="checkbox"/>	Microsoft Excel	Deskinfo..xls	-
<input type="checkbox"/>	Microsoft Excel	Deskinfo..xls	-

TotalDocuments | File Size

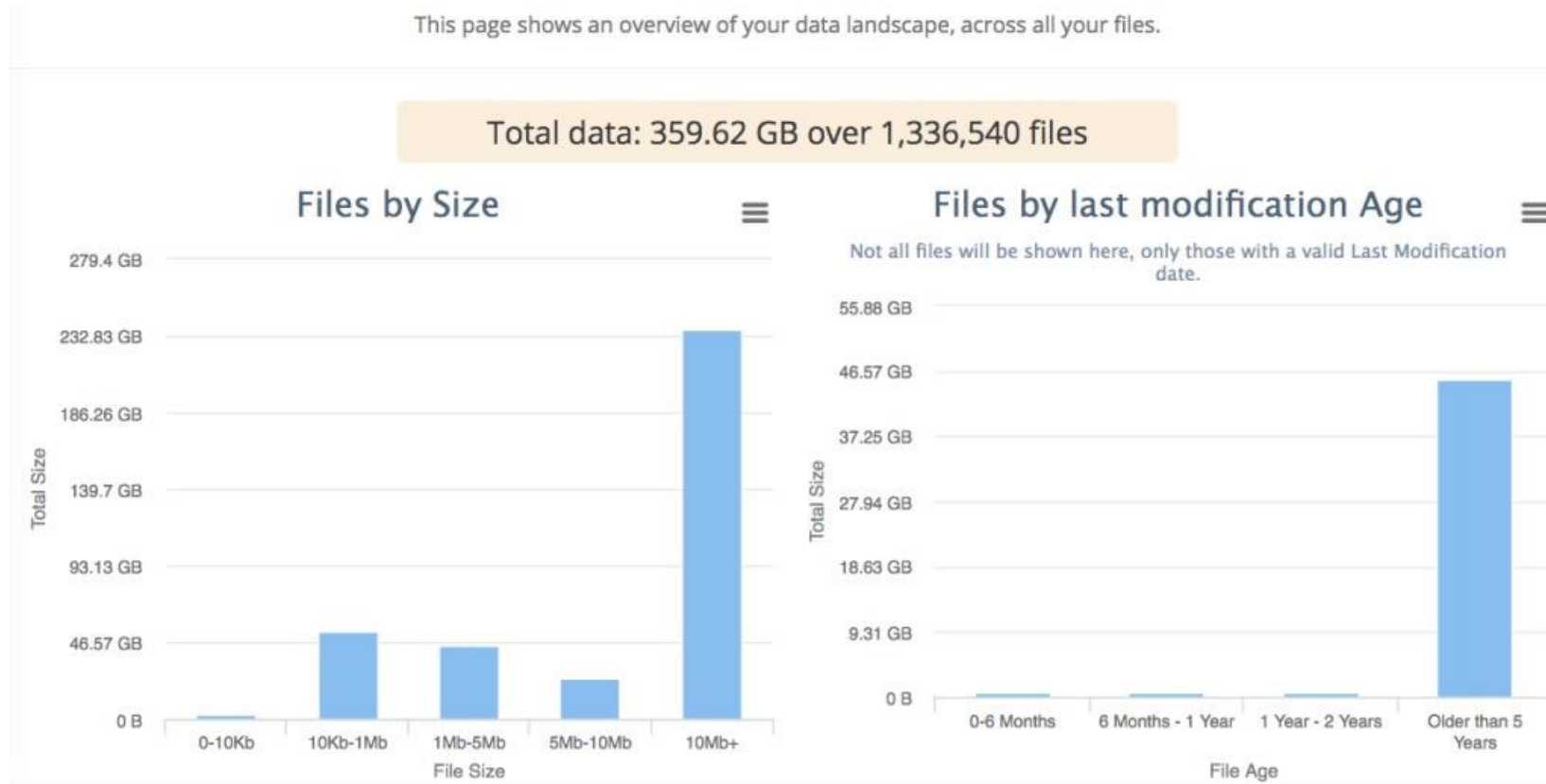
15



[illegible]



Information Intelligence; **understand**





Information Intelligence; **act**

Securely Delete data
from legacy arrays
from active LUNs
from Windows file servers





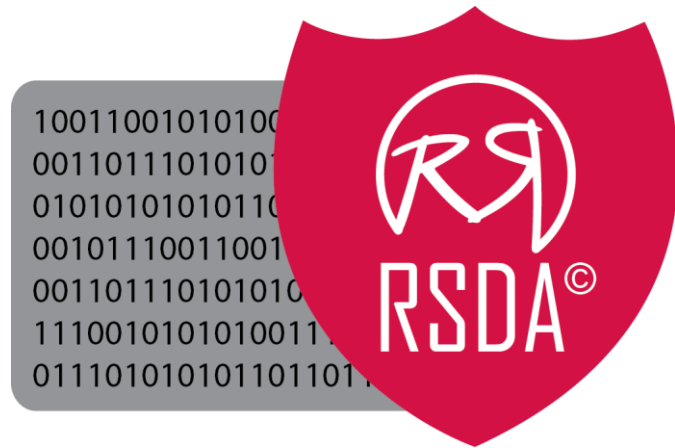
Information Intelligence; **act**



Strive for full compliance



Strive for full compliance



Know your data content before you invest in expensive security software

Steve Withers:

stephen.withers@reciprocalgroup.co.uk
07808 870492

Dave Knock:

dave.knock@reciprocalgroup.co.uk
07701 288824







Cyber compliance: Convergence of Cyber and Compliance Risk

**Q4-2016 ITF Security Matters Forum
15 December 2016**

Alan Calder
IT Governance Ltd
www.itgovernance.co.uk

Introduction



- Alan Calder
- Founder – IT Governance Ltd
- *IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002, 6th Edition* (Open University textbook)
- www.itgovernance.co.uk/shop/p-772-it-governance-an-international-guide-to-data-security-and-iso27001iso27002.aspx

IT Governance Ltd: GRC One-Stop-Shop



Thought Leaders
Specialist publisher



Implementation toolkits



ATO



Consultants



Software and e-learning



Distribution

IT governance, risk and compliance

Cyber resilience

Governance and
risk management

Information security
and
ISO 27001

Business
continuity
management
and
ISO 22301

IT
governance

Service
management

Project
management

PCI DSS

Penetration
testing

Data
protection

Incident
response
management

COBIT®

ITIL®
and
ISO 20000

PRINCE2®
and
PMBOK®

Consultancy and
certification

Security testing

Training and
qualifications

Software tools

Toolkits and
publications

Point solutions that integrate.....



Agenda



- Global backdrop: today's cyber threat environment
- EU GDPR
- NIS
- Cyber assurance
- 7-Step action plan

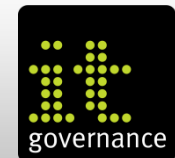
Cyber disconnect



- Most organizations are 'confident' in their cyber defences
- 70% of organizations say:
 - Cyber security completely embedded in their processes
 - Cyber security a board-level concern, with top executive focus
- However:
 - Organizations face 100+ targeted attacks per year
 - 1/3 are successful – that's 2 or 3 per month!
 - Most breaches are discovered by outsiders!

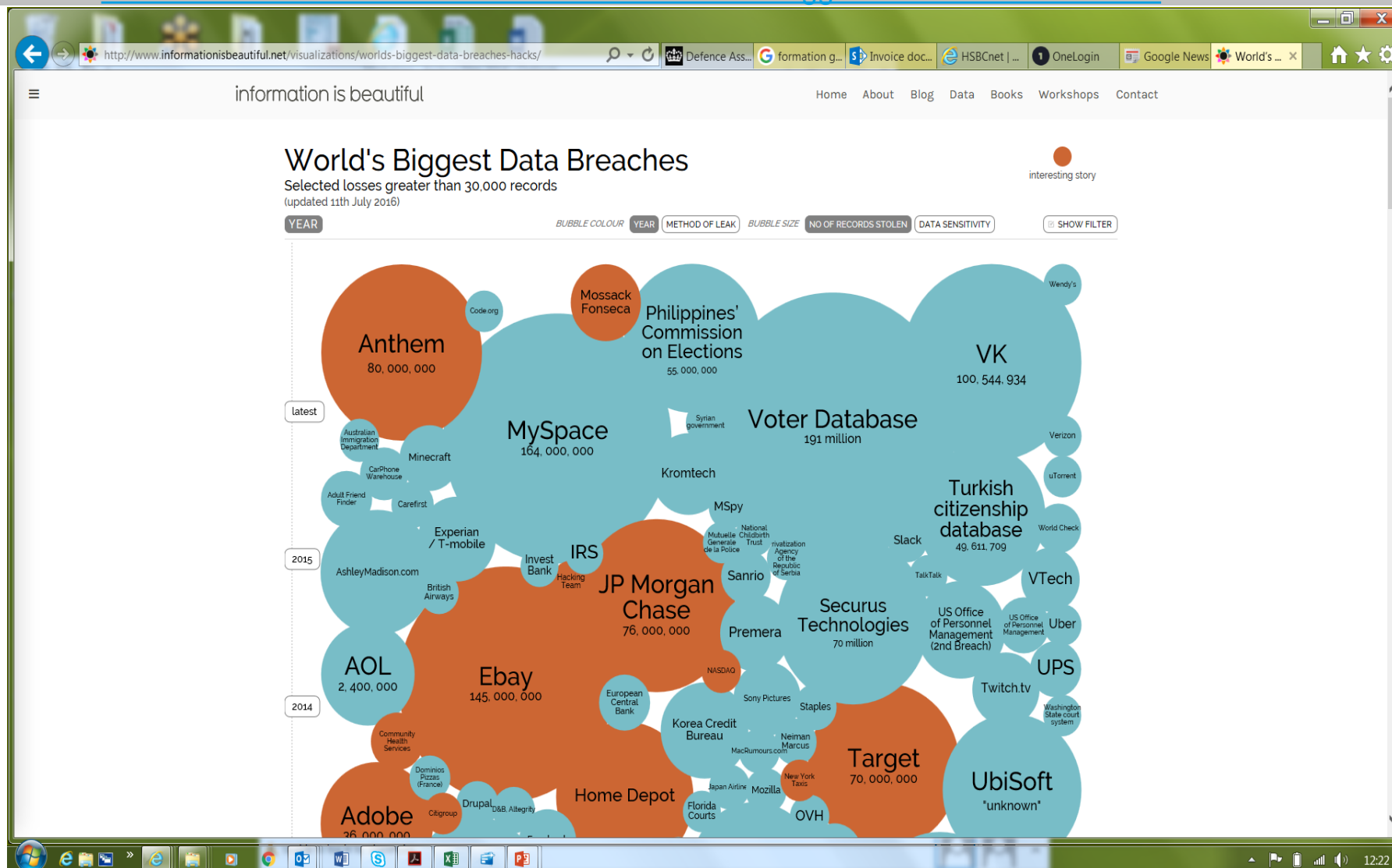
(Accenture: Facing the Cybersecurity Conundrum 2016)

Cyber attack environment



Massive data breaches

- www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



Cyber risk – an overview



Attackers



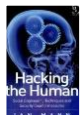
Hacktivists



Terrorists



Opportunists



Criminals



Competitors

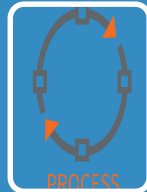


Enemies

Weaknesses



People



Process



Technology

Assets

IP

Card data

PII

Money

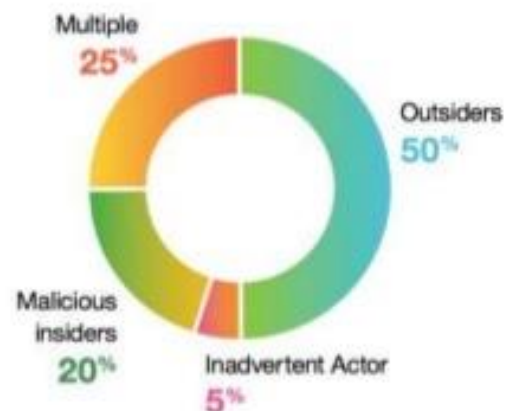
Reputation

Commercial
Info

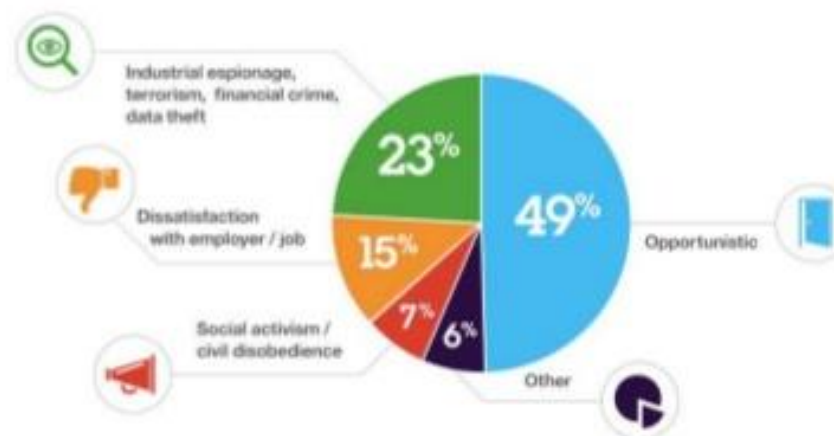
Threats

Threats: Who Attacks and Why?

Categories of Attackers



Attacker Motivation



From IBM's 2013 Cyber Security Intelligence Index

Cyber threat evolution



Cyber risks



- Digital Information is at the heart of cyber crime
 - Key assets at risk:
 - High value research and technology – eg energy technology, advanced engineering, communications technology
 - Politically/commercially sensitive data – eg product development, climate modelling, shipping/manifest information
 - Sensitive internal information: eg PII (customers, passengers and staff), financial data (eg bank accounts, payment card data, identity theft)
 - High value physical assets under digital control
 - Key challenges:
 - Multiplicity of threat actors: nation-states, competitors, criminals, terrorists, hackers
 - Complex supply chains
 - Multiple, mobile and remote access connection requirements
 - Rapid technology evolution
 - Inadequate staff awareness
 - Process deficits

Security breach levels are rising



Security breach levels continue to rise. Last year in the UK:

- 90% of large organisations reported suffering a security breach, up from 81% a year before.
- 74% of small businesses had a security breach, up from 60% a year before.

Source: BIS/PwC 2015 Information Security Breaches Survey

Cost of cyber crime is rising



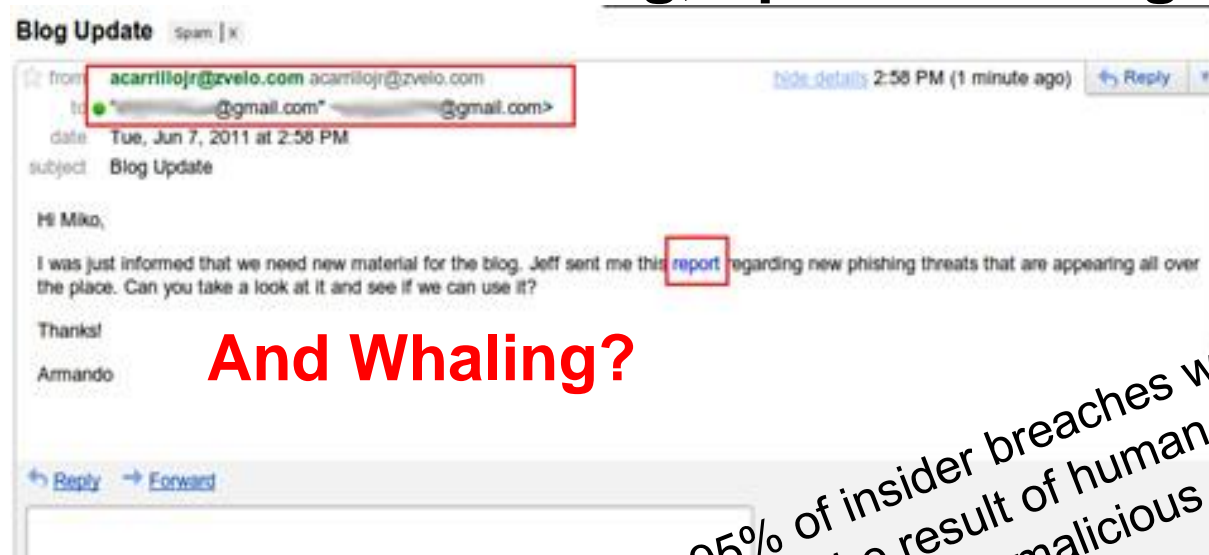
The average cost of a data breach for businesses in the UK is £2.37 million.

Source: IBM/Ponemon Institute 2015 Cost of Data Breach Study: United Kingdom

Hacking the Human



Phishing, Spear Phishing



And Whaling?

95% of insider breaches were found to be the result of human error, such as clicking on malicious links in phishing emails.

Cryptolocker & Ransom-ware



Self-installs

- Phishing emails
- Compromised websites
- Existing malware

Can Encrypt:

- shared network drives,
- USB drives,
- external hard drives,
- network file shares,
- some cloud storage drives

Cost of Decryption Key: €300 – or 2 Bitcoins

Cryptolocker – 240,000 infected computers since Oct 2013
£16 million in ransoms.....

GameOverZeuS – steals online banking passwords
\$100 million of income...

APT: Multi-channel attack

Advanced Persistent Threat (APT): The Uninvited Guest

How attackers remain in your network harvesting information and avoiding detection over time

1. INCURSION

Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems and people.

2. DISCOVERY

Once in, the attackers stay “low and slow” to avoid detection. They then map the organization’s defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success.

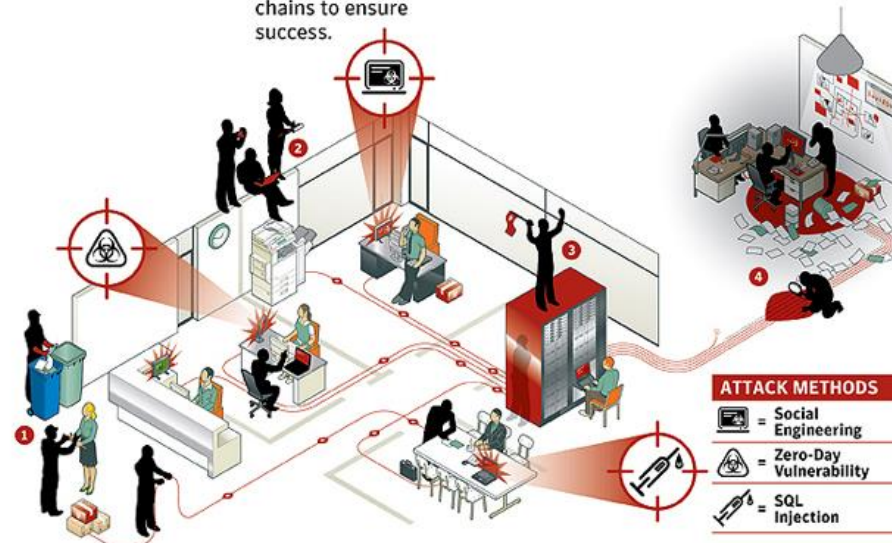
3. CAPTURE

Attackers access unprotected systems and capture information over an extended period.

They may also install malware to secretly acquire data or disrupt operations.

4. EXFILTRATION

Captured information is sent back to attack team’s home base for analysis and further exploitation fraud—or worse.



Small supply chain businesses are popular with hackers



- Many small businesses are on shared servers. This multiplies the potential access points for a hacker to exploit.
- Small to mid-size businesses usually don't have an IT department that keeps server hardware and software up-to-date.
- Website versions and plug-ins are often out-of-date and easily hacked.
- Small to mid-size companies usually don't have internal security practices, so passwords and access are easily compromised.
- Small business websites are often built on common, open-source frameworks. These frameworks are popular to hackers because there are so many and the same weaknesses can be exploited across all of them.
- (Executionists Blog)

The stakes are high!



The potential impacts of cyber attack:

- Loss of life
- Loss of high-value physical assets
- Climate destruction
- Direct financial loss from theft or fraud.
- Indirect loss from recovery & remediation costs
- Loss of customer information or intellectual property.
- Possible fines from legal and regulatory bodies (e.g. Information Commissioner).
- Loss of reputation through 'word of mouth' and adverse press coverage.
- Survival of the organisation itself.

Demands for assurance


74% of respondents say their customers prefer dealing with suppliers with proven cyber security credentials, while 50% say their company has been asked about its information security measures by customers in the past 12 months.

EU GDPR


**What the new
EU GDPR
means in 1 minute**

The EU GDPR will increase privacy for individuals and give regulatory authorities greater powers to take action against businesses that breach the new laws.
Here's what it means for your business:

Tough penalties:
fines of up to
4% of annual global revenue
or
€20 million,
whichever is greater.

A green money bag with a drawstring top sits on a black platform scale with a white dial and a blue needle.

The regulation also applies to **non-EU companies** that process personal data of individuals in the EU.

A world map with black landmasses and white oceans. Blue curved arrows point from North America, Asia, and Australia towards Europe, which is highlighted in yellow.

Complete overhaul of data protection framework

Covers all forms of PII, including biometric, genetic and location data

Applies across all member states of the EU

In force on 25th May 2018

GDPR – data breaches



- ***Mandatory data breach reporting – within 72 hours***
 - Describe actions being taken to
 - Address the breach
 - Mitigate the consequences
 - Data subjects contacted ‘without undue delay’
 - Unnecessary if appropriate protection is already in place
 - Consider encryption for all mobile devices, for all databases, and for email
 - Penetration testing to identify potential attack vectors should be standard
- Failure to report within 72 hours must be explained

NIS: Network & Information Security Directive



- Applies to:
 - ‘Essential services’– eg CNI, Finance, Health, Utilities, Transport, Energy, Food, Marine etc
 - Digital Service Providers
- Translated into national law by May 2018
- Increase intra-EU cooperation, national CSIRT network
- Adopt technical and organizational measures appropriate to risk:
 - Ensure the security of systems and facilities
 - Processes for Incident handling
 - Business continuity management
 - Monitoring, auditing and testing
 - Compliance with international standards
- Penalties for infringement must be ‘effective, proportionate and dissuasive’.

What can you do to stay safe: Cyber Essentials Scheme



1. Boundary Firewalls & Internet Gateways
2. Secure Configuration
3. Access Control
4. Malware Protection
5. Patch Management

ONLY £300
These are the five basic controls that any organization should implement to mitigate the risk from common internet-borne threats.



Cyber Essentials vs Cyber Essentials Plus



Cyber Essentials:

- *Self Assessment Questionnaire*
- *Attestation of Compliance*
- *External vulnerability scan*

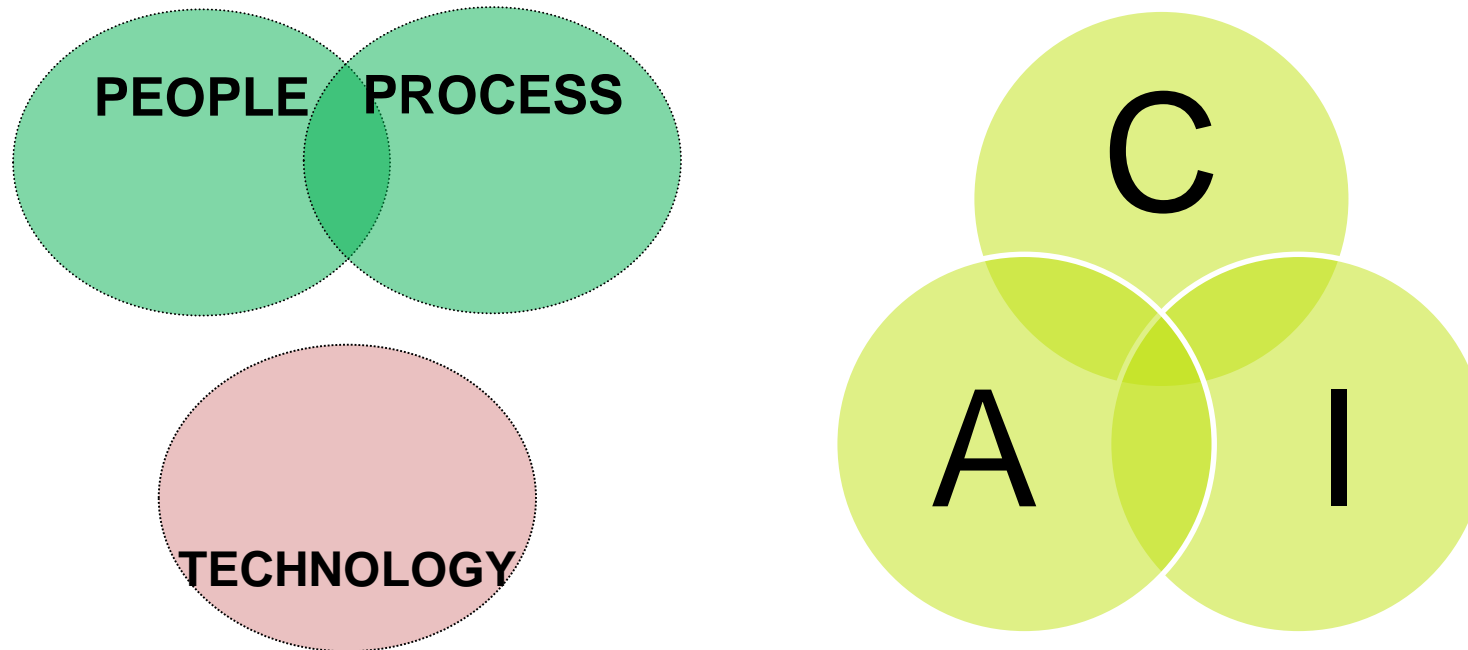
Cyber Essentials Plus

- *As for Cyber Essentials, plus*
- *Onsite test of device configurations*

Independent Certification
CREST-accredited



Key considerations



- Management-driven
- Business-focused
- Risk appetite-based
- Enterprise-orientated
- Continual improvement

Convergence: cyber security assurance



- ISO/IEC 27001:2013
 - Is an international standard
 - already meets the “appropriate technical and organizational measures” requirement
 - Is widely recognised and adopted
- Provides assurance to the board that data security is being managed in accordance with business, contractual and regulatory requirements
 - Information security/data protection policies
 - Audit, monitoring and review
- Manage ALL information assets and all information security within the organization – protecting against ALL threats

Cyber resilience



- Resilience:
 - “the ability to rapidly adapt, protect assets and respond to risks...”
- Business Resilience:
 - “the ability to rapidly adapt, protect business assets, respond to business disruptions and maintain continuous business operations..”
 - Contains both BCM and DR
 - Implies mitigation capability
- Cyber-resilience
 - “the ability to repel cyber attacks while protecting critical business assets, rapidly adapting and responding to business disruptions and maintaining continuous business operations..”

7-Step cyber-resilience strategy

1. Governance, clear policies, leadership
2. Business, regulatory and contractual requirements
3. Integrated risk assessment, BIA, DPIA
 - Assets AND Processes
4. Secure the cyber perimeter & endpoints; defence in depth
5. Train all staff – skills, competence, awareness
6. Develop and test a security incident response and escalation plan
7. Audit, monitor, test, continually improve

Start with ISO 27001 & ISO 22301

Questions?

acalder@itgovernance.co.uk

0845 070 1750

www.itgovernance.co.uk



'Security Matters' forums are managed by Insurance Technology Forums Ltd, the specialist host of IT and security briefings for decision-makers in today's Lloyd's and London insurance market.