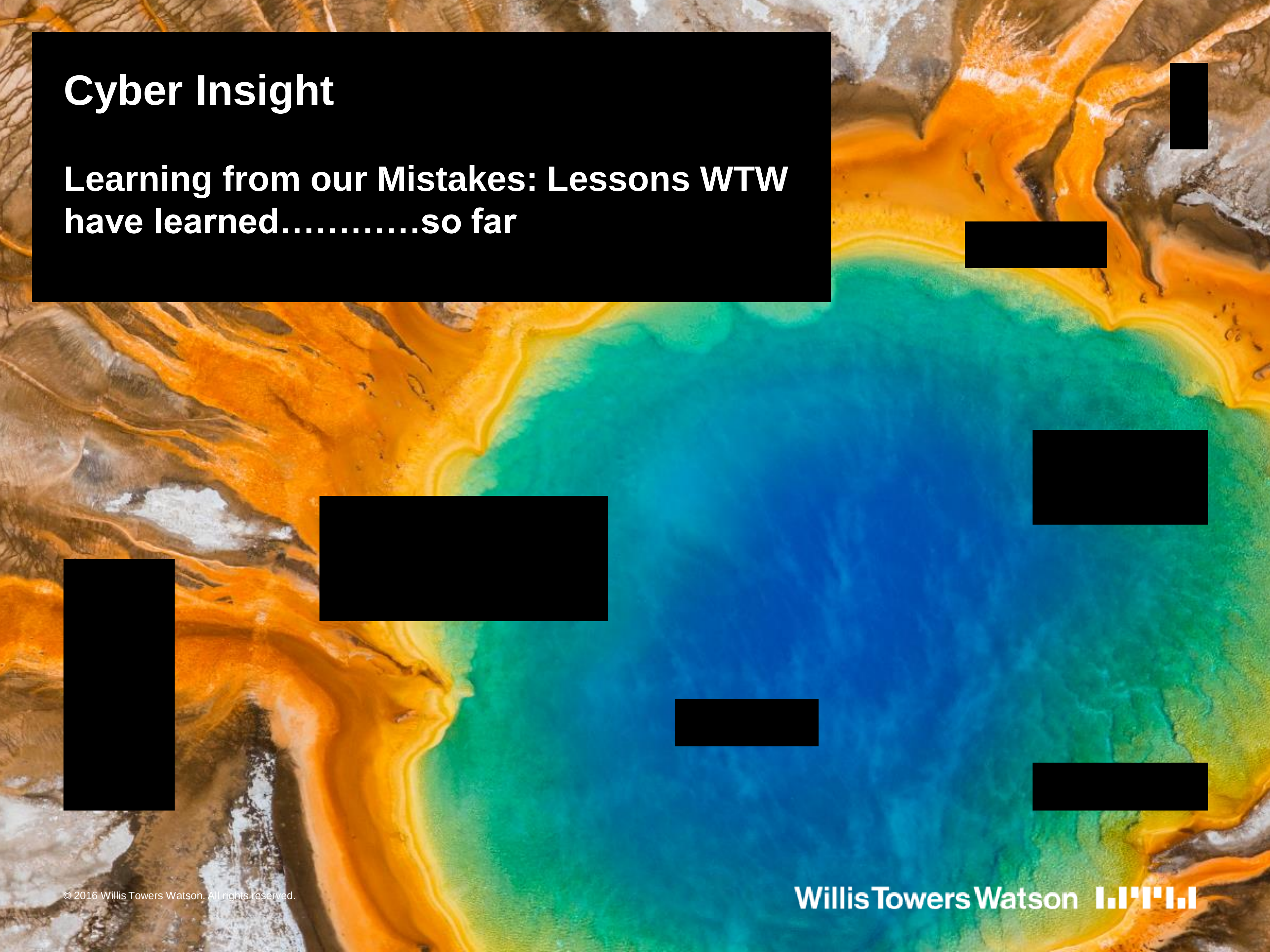


Cyber Insight

Learning from our Mistakes: Lessons WTW have learned…………so far

[redacted]

[redacted]

[redacted]

[redacted]

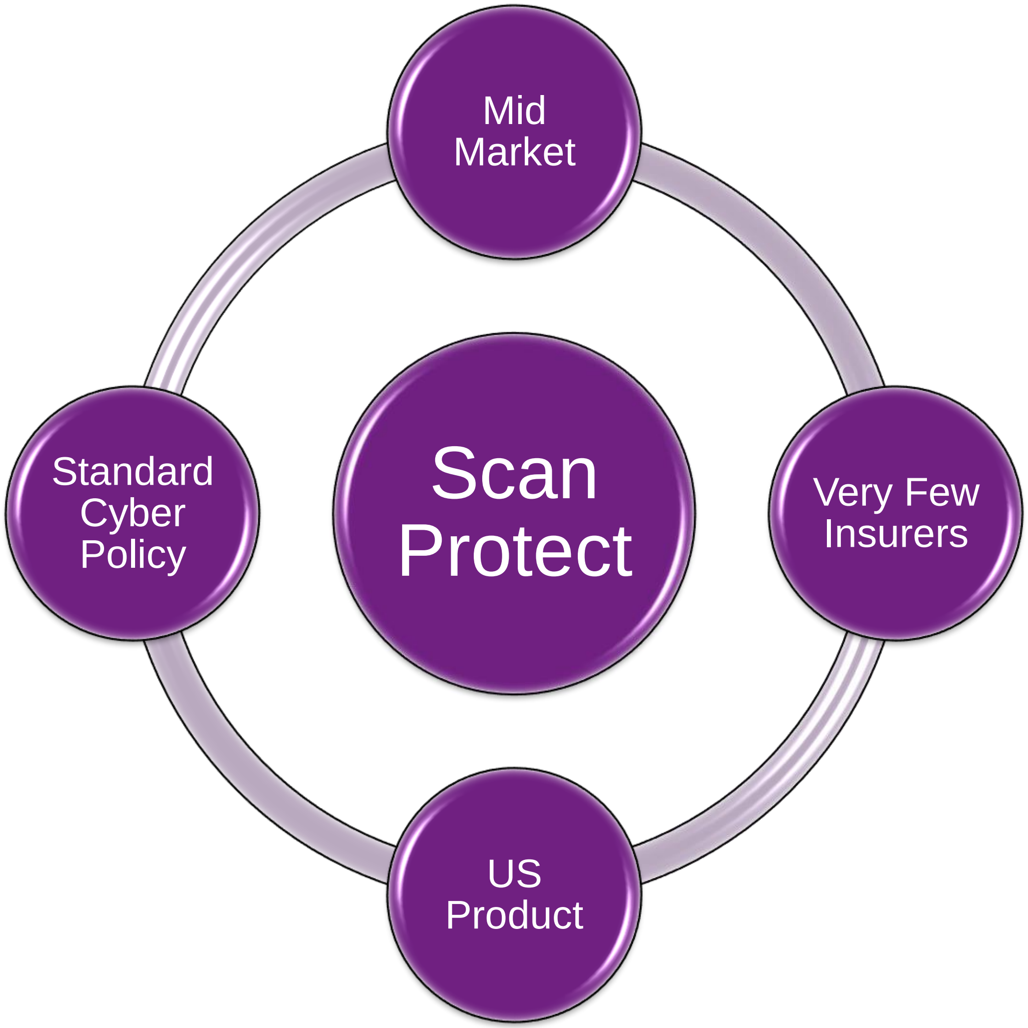
[redacted]

[redacted]

[redacted]

Willis Towers Watson

Our first attempt……….2011



Scan Protect

Mid Market

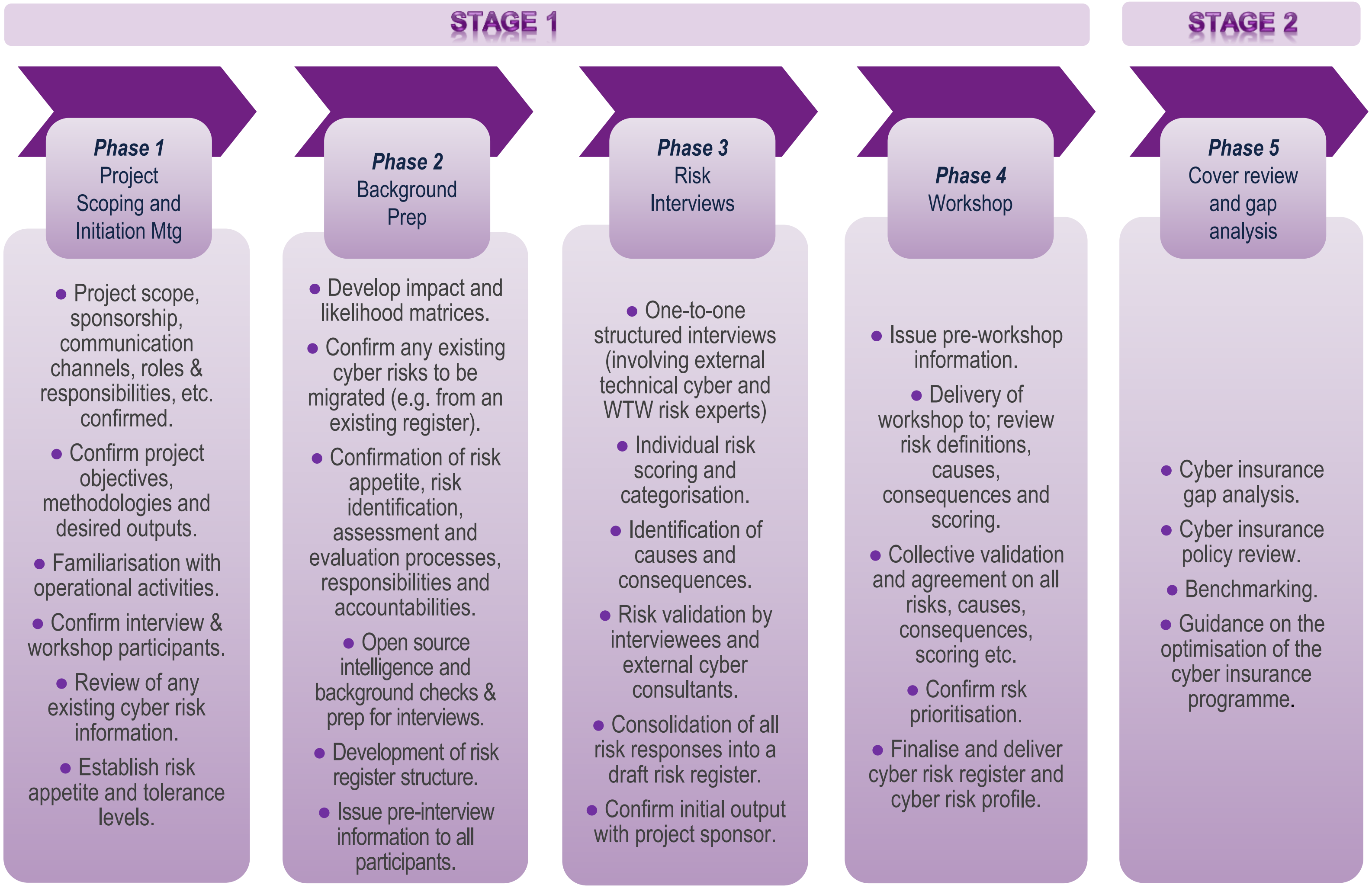
Very Few Insurers

US Product

Standard Cyber Policy

Cyber Risk and Insurance Assessment

The 2-Stage Process



STAGE 1

Phase 1
Project Scoping and Initiation Mtg

- Project scope, sponsorship, communication channels, roles & responsibilities, etc. confirmed.
- Confirm project objectives, methodologies and desired outputs.
- Familiarisation with operational activities.
- Confirm interview & workshop participants.
- Review of any existing cyber risk information.
- Establish risk appetite and tolerance levels.

Phase 2
Background Prep

- Develop impact and likelihood matrices.
- Confirm any existing cyber risks to be migrated (e.g. from an existing register).
- Confirmation of risk appetite, risk identification, assessment and evaluation processes, responsibilities and accountabilities.
- Open source intelligence and background checks & prep for interviews.
- Development of risk register structure.
- Issue pre-interview information to all participants.

Phase 3
Risk Interviews

- One-to-one structured interviews (involving external technical cyber and WTW risk experts)
- Individual risk scoring and categorisation.
- Identification of causes and consequences.
- Risk validation by interviewees and external cyber consultants.
- Consolidation of all risk responses into a draft risk register.
- Confirm initial output with project sponsor.

Phase 4
Workshop

- Issue pre-workshop information.
- Delivery of workshop to; review risk definitions, causes, consequences and scoring.
- Collective validation and agreement on all risks, causes, consequences, scoring etc.
- Confirm rsk prioritisation.
- Finalise and deliver cyber risk register and cyber risk profile.

STAGE 2

Phase 5
Cover review and gap analysis

- Cyber insurance gap analysis.
- Cyber insurance policy review.
- Benchmarking.
- Guidance on the optimisation of the cyber insurance programme.

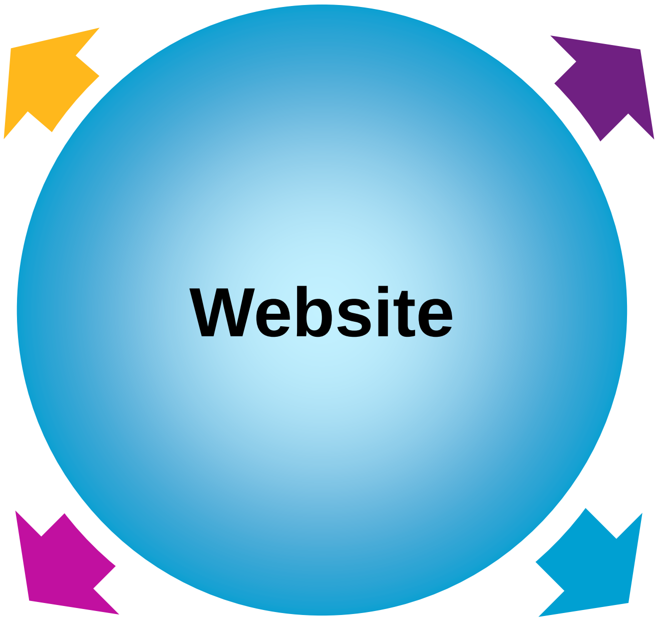
OPEN SOURCE INTELLIGENCE……………….

PEOPLE:

- EMAIL ADDRESS
- SOCIAL MEDIA
- INTERESTS
- PHONE NUMBERS
- FAMILY
- PERSONAL DETAILS
- PHOTOGRAPHS

LOCATIONS:

- PHYSICAL SITES
- SERVICE PROVIDERS



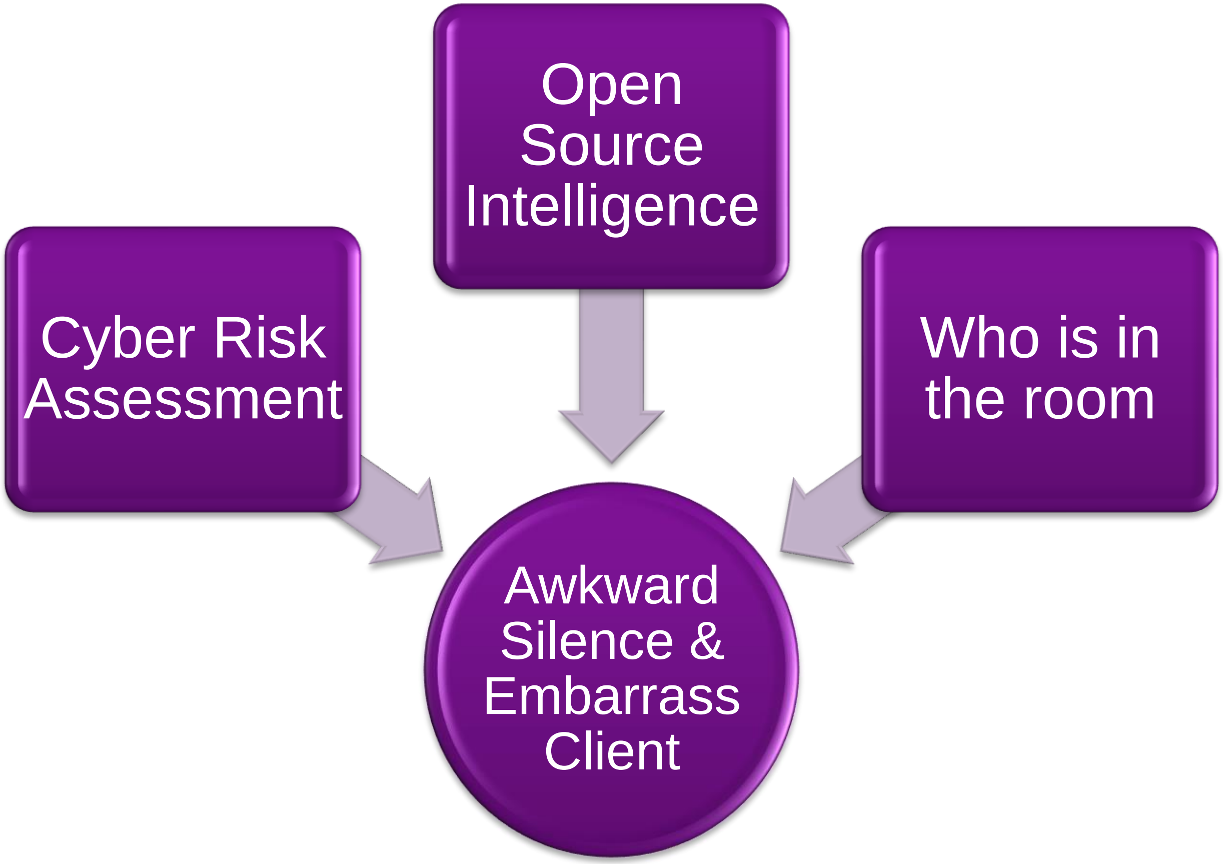
DOCUMENTS:

- PROCEDURES
- IP
- CONTRACTS
- STRUCTURE
- STAFF NAMES

S/W & O/S:

- NETWORK
- VULNERABILITIES
- EQUIPMENT

In our Haste to help……..



Open Source Intelligence

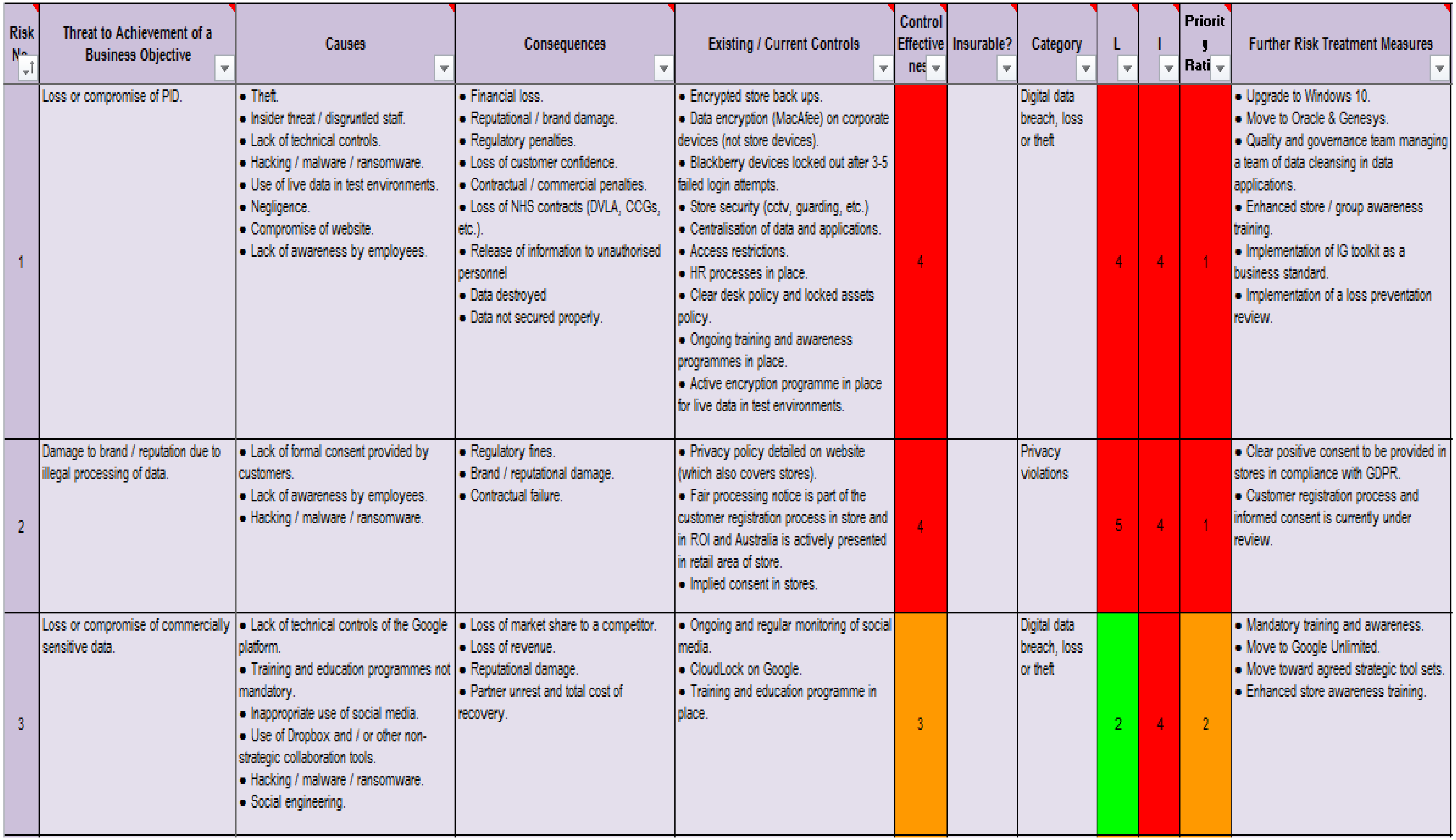
Cyber Risk Assessment

Who is in the room

Awkward Silence & Embarrass Client

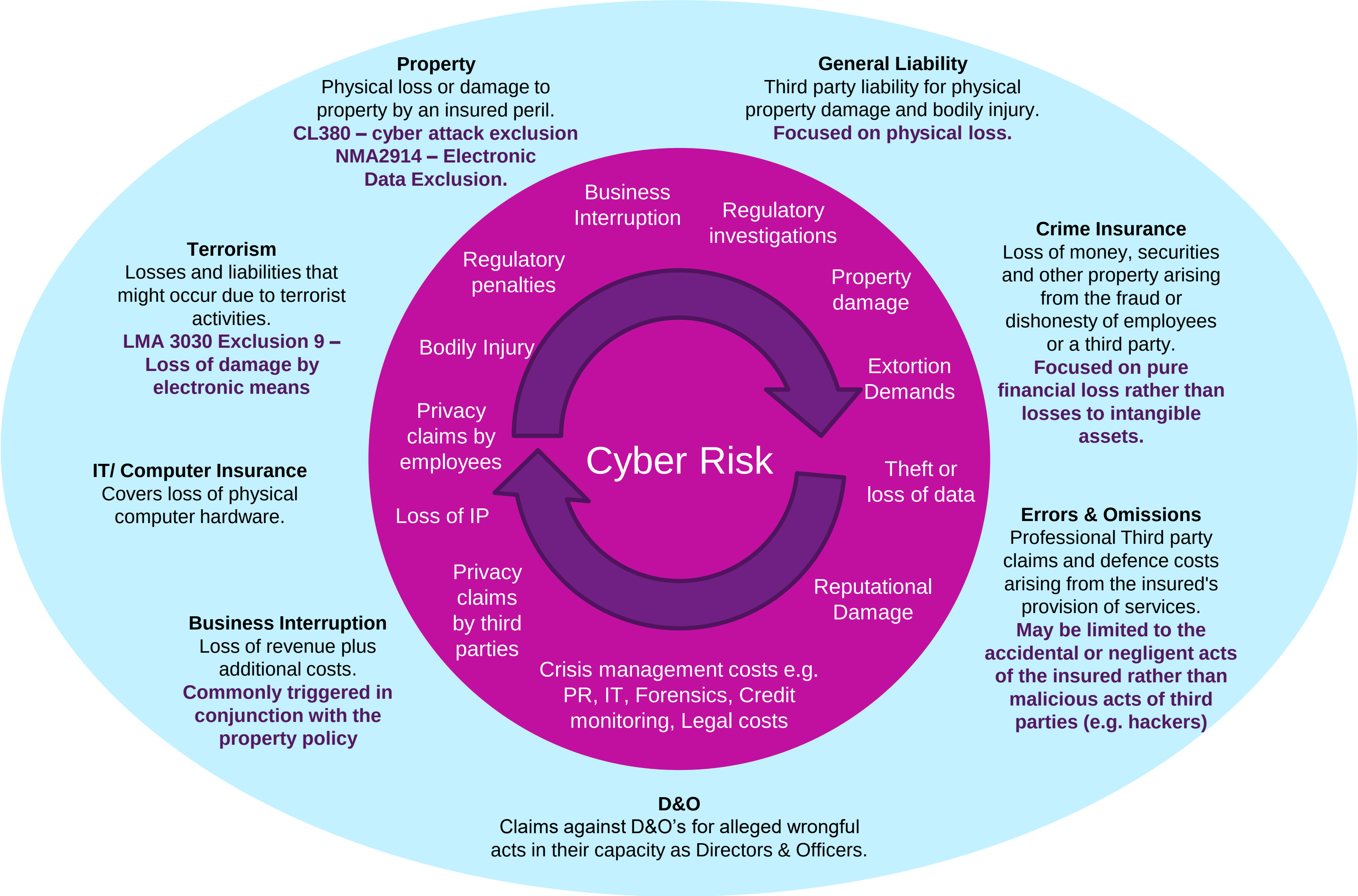
Cyber Risk and Insurance Assessment

Example Risk Register



Risk No	Threat to Achievement of a Business Objective	Causes	Consequences	Existing / Current Controls	Control Effective nes	Insurable?	Category	L	I	Priorit y Rati	Further Risk Treatment Measures
1	Loss or compromise of PID.	• Theft. • Insider threat / disgruntled staff. • Lack of technical controls. • Hacking / malware / ransomware. • Use of live data in test environments. • Negligence. • Compromise of website. • Lack of awareness by employees.	• Financial loss. • Reputational / brand damage. • Regulatory penalties. • Loss of customer confidence. • Contractual / commercial penalties. • Loss of NHS contracts (DVLA, CCGs, etc.). • Release of information to unauthorised personnel • Data destroyed • Data not secured properly.	• Encrypted store back ups. • Data encryption (MacAfee) on corporate devices (not store devices). • Blackberry devices locked out after 3-5 failed login attempts. • Store security (cctv, guarding, etc.) • Centralisation of data and applications. • Access restrictions. • HR processes in place. • Clear desk policy and locked assets policy. • Ongoing training and awareness programmes in place. • Active encryption programme in place for live data in test environments.	4		Digital data breach, loss or theft	4	4	1	• Upgrade to Windows 10. • Move to Oracle & Genesys. • Quality and governance team managing a team of data cleansing in data applications. • Enhanced store / group awareness training. • Implementation of IG toolkit as a business standard. • Implementation of a loss prevention review.
2	Damage to brand / reputation due to illegal processing of data.	• Lack of formal consent provided by customers. • Lack of awareness by employees. • Hacking / malware / ransomware.	• Regulatory fines. • Brand / reputational damage. • Contractual failure.	• Privacy policy detailed on website (which also covers stores). • Fair processing notice is part of the customer registration process in store and in ROI and Australia is actively presented in retail area of store. • Implied consent in stores.	4		Privacy violations	5	4	1	• Clear positive consent to be provided in stores in compliance with GDPR. • Customer registration process and informed consent is currently under review.
3	Loss or compromise of commercially sensitive data.	• Lack of technical controls of the Google platform. • Training and education programmes not mandatory. • Inappropriate use of social media. • Use of Dropbox and / or other non-strategic collaboration tools. • Hacking / malware / ransomware. • Social engineering.	• Loss of market share to a competitor. • Loss of revenue. • Reputational damage. • Partner unrest and total cost of recovery.	• Ongoing and regular monitoring of social media. • CloudLock on Google. • Training and education programme in place.	3		Digital data breach, loss or theft	2	4	2	• Mandatory training and awareness. • Move to Google Unlimited. • Move toward agreed strategic tool sets. • Enhanced store awareness training.

Cyber risk insurance implications – Mind the GAP!



Property
Physical loss or damage to property by an insured peril.
CL380 – cyber attack exclusion
NMA2914 – Electronic Data Exclusion.

General Liability
Third party liability for physical property damage and bodily injury.
Focused on physical loss.

Terrorism
Losses and liabilities that might occur due to terrorist activities.
LMA 3030 Exclusion 9 – Loss of damage by electronic means

Crime Insurance
Loss of money, securities and other property arising from the fraud or dishonesty of employees or a third party.
Focused on pure financial loss rather than losses to intangible assets.

IT/ Computer Insurance
Covers loss of physical computer hardware.

Errors & Omissions
Professional Third party claims and defence costs arising from the insured's provision of services.
May be limited to the accidental or negligent acts of the insured rather than malicious acts of third parties (e.g. hackers)

Business Interruption
Loss of revenue plus additional costs.
Commonly triggered in conjunction with the property policy

D&O
Claims against D&O's for alleged wrongful acts in their capacity as Directors & Officers.

Cyber Risk

Business Interruption

Regulatory investigations

Regulatory penalties

Property damage

Bodily Injury

Extortion Demands

Privacy claims by employees

Theft or loss of data

Loss of IP

Privacy claims by third parties

Reputational Damage

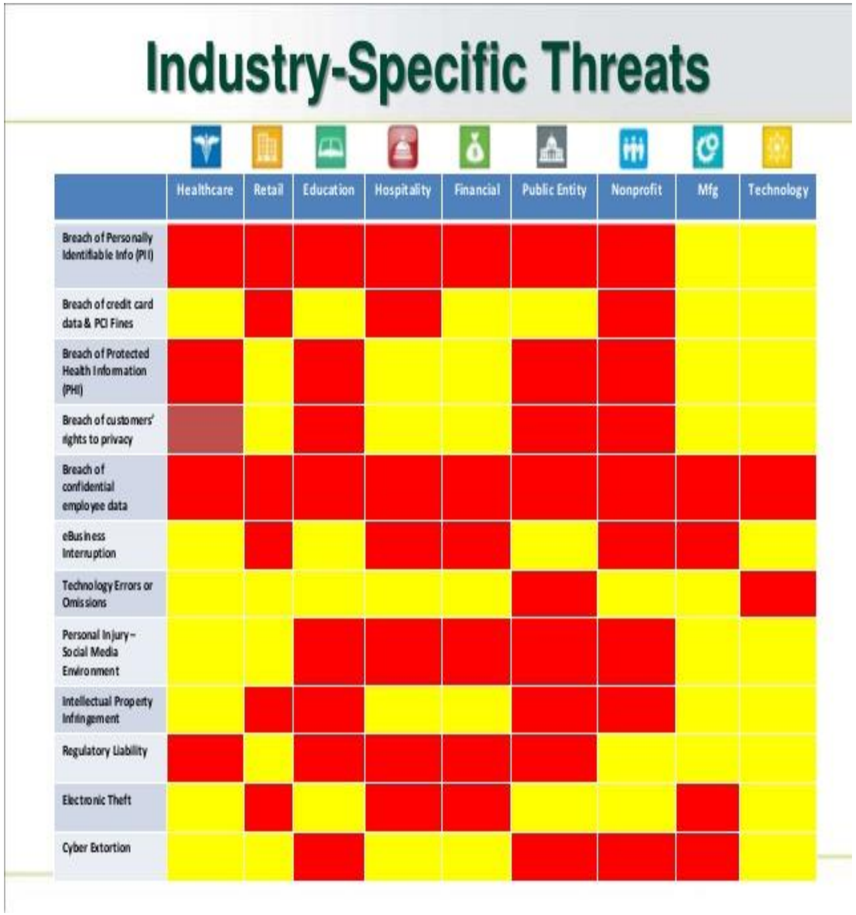
Crisis management costs e.g. PR, IT, Forensics, Credit monitoring, Legal costs

Industry Specific

CYBER RISK WILL DIFFER BY INDUSTRY VERTICAL

To understand your own firm's cyber exposure – you must understand that of its industry sector:

- Health sector: loss or theft of medical data and (increasingly) system malfunction / denial of service attack
- Professional/managerial: theft of commercially sensitive information and personal data
- Financial services: theft of money and personal financial data
- Education: theft of sensitive personal data, confidential information and R & D
- Retail: business interruption and theft of personal financial data
- Marine: physical damage, cyber extortion and theft of confidential information
- Air/Air traffic control: denial of service attack/cyber extortion
- Newspapers: theft of sensitive information, multimedia risk/defamation.



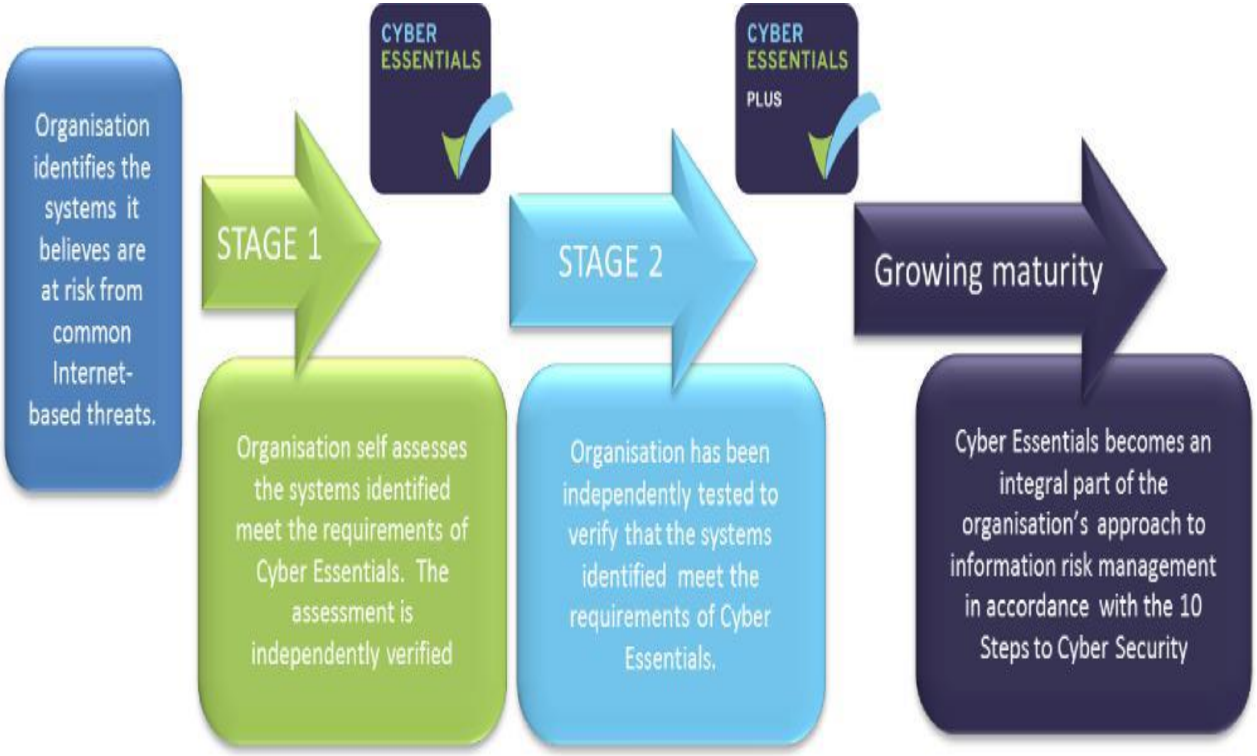
Industry-Specific Threats

	Healthcare	Retail	Education	Hospitality	Financial	Public Entity	Nonprofit	Mfg	Technology
Breach of Personally Identifiable Info (PII)	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨
Breach of credit card data & PCI Fines	🟨	🟥	🟨	🟥	🟨	🟨	🟥	🟨	🟨
Breach of Protected Health Information (PHI)	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟨	🟨
Breach of customers' rights to privacy	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟨	🟨
Breach of confidential employee data	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
eBusiness Interruption	🟨	🟥	🟨	🟥	🟥	🟨	🟥	🟥	🟨
Technology Errors or Omissions	🟨	🟨	🟨	🟨	🟨	🟥	🟨	🟨	🟥
Personal Injury – Social Media Environment	🟨	🟨	🟥	🟥	🟥	🟥	🟥	🟨	🟨
Intellectual Property Infringement	🟨	🟥	🟥	🟨	🟨	🟥	🟥	🟨	🟨
Regulatory Liability	🟥	🟨	🟥	🟥	🟥	🟥	🟨	🟨	🟨
Electronic Theft	🟨	🟥	🟨	🟥	🟥	🟨	🟨	🟥	🟨
Cyber Extortion	🟨	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟨

CYBER ESSENTIALS

Cyber Essentials concentrates on five key controls:

- Boundary firewalls and internet gateways
- Secure configuration
- Access control
- Malware protection
- Patch management



Organisation identifies the systems it believes are at risk from common Internet-based threats.

STAGE 1

CYBER ESSENTIALS

Organisation self assesses the systems identified meet the requirements of Cyber Essentials. The assessment is independently verified

STAGE 2

CYBER ESSENTIALS PLUS

Organisation has been independently tested to verify that the systems identified meet the requirements of Cyber Essentials.

Growing maturity

Cyber Essentials becomes an integral part of the organisation's approach to information risk management in accordance with the 10 Steps to Cyber Security

What Limit Should we Buy ?

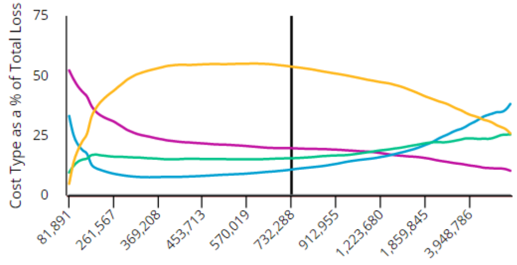
As much as you can afford

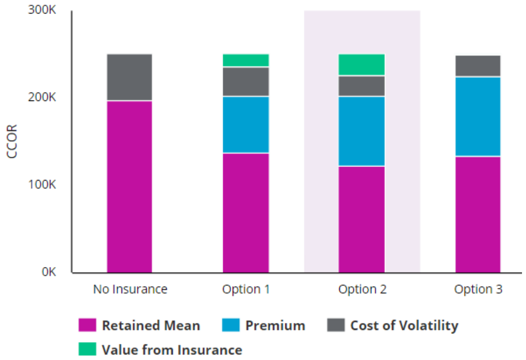
Cyber Quantified

This latest innovation in cyber risk prediction evaluates your firm's complete cyber loss potential with decision support to optimise risk management strategy.

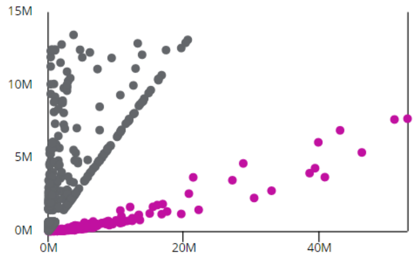
Going beyond other cyber risk models in the industry, Cyber Quantified interactively incorporates network outage risk in addition to privacy breach liability. Cyber Quantified's refined evaluation of your organisation's comprehensive risk includes:

- Dynamic and customisable technology allowing for collaborative sensitivity testing with **instantaneous results**
- **Thorough quantification of cyber risk**: Frequency and Severity of both privacy breach and network outage
- Visually compelling **data driven decision support** guide insurance strategy via range of a single incident, CCOR, and impact of insurance.
- Facilitates strategic and **tactical engagement of the insurance marketplace**
- Concise and compelling output for **efficient communication** with internal stakeholders

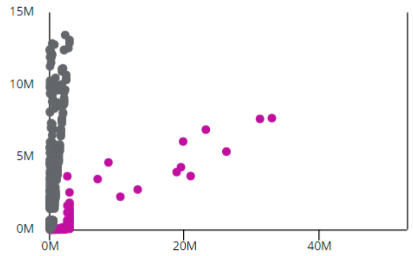




No Insurance



With insurance



Inquiries: CyberQuantified@WillisTowersWatson.com

WTW 2017 Cyber Risk Survey

Cyber security is viewed as a fundamental challenge and a top priority for organisations.

Many companies feel they are on the right track in terms of data privacy and cyber security risk management.

But most recognise that this is a journey and many are looking to **create a culture of cyber security** in their organisation.

Many threats exist around **employee behaviours** and the vulnerabilities around human error will be a top priority over the next three years.

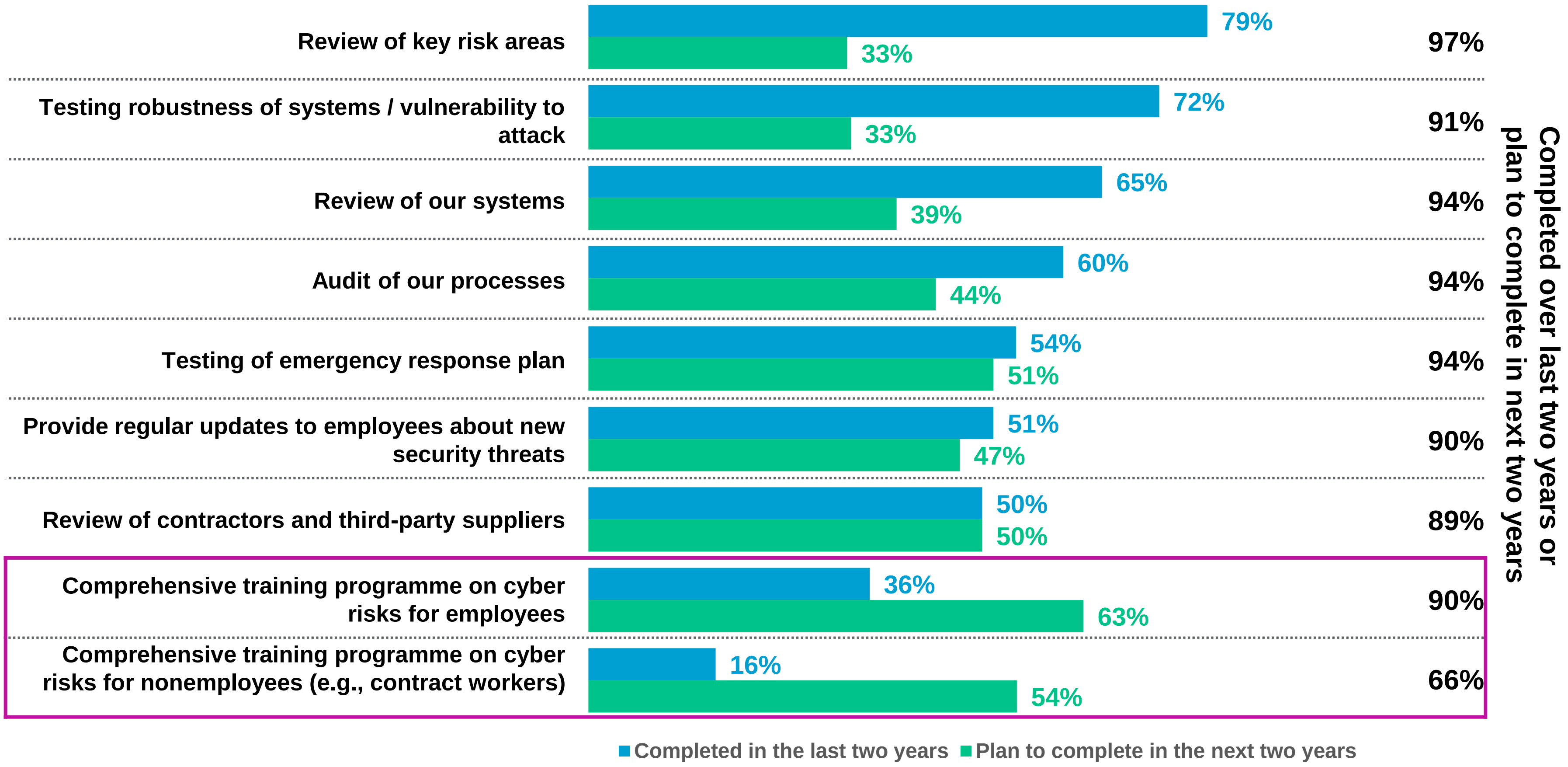
Immediate priorities are:

- **Training for employees and contractors**
- Reviewing the cyber insurance gap and adding coverage

Source: 2017 WTW Cyber Risk Survey, employer survey, UK.

The initial focus was chiefly on technology, but increasingly this will shift to employee behaviour and operating procedures

Has your organisation completed in the last two years, or does it plan to complete in the next two years, any of the following cyber risk related activities?



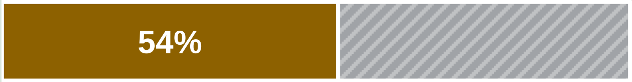
Source: 2017 WTW Cyber Risk Survey, employer survey, UK

Awareness of social engineering risk among employees needs to be enhanced

Thinking about how you use technology, do you…?

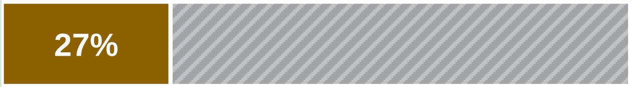
Protection from social engineering attacks

Disable features that let you auto-save passwords on your personal computing devices



(% of 'Yes')

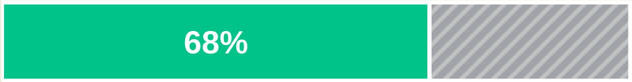
Purchase a personal identity theft protection service



(% of 'Yes')

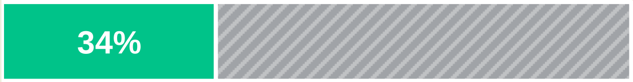
Vulnerabilities to social engineering attacks

Only change the password on my work computer when prompted



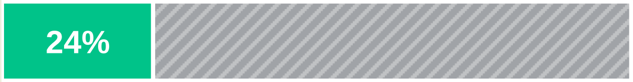
(% of 'Strongly agree' or 'Agree')

Share personal information (e.g., date of birth, employer name, job title) in profiles on social media sites



(% of 'Yes')

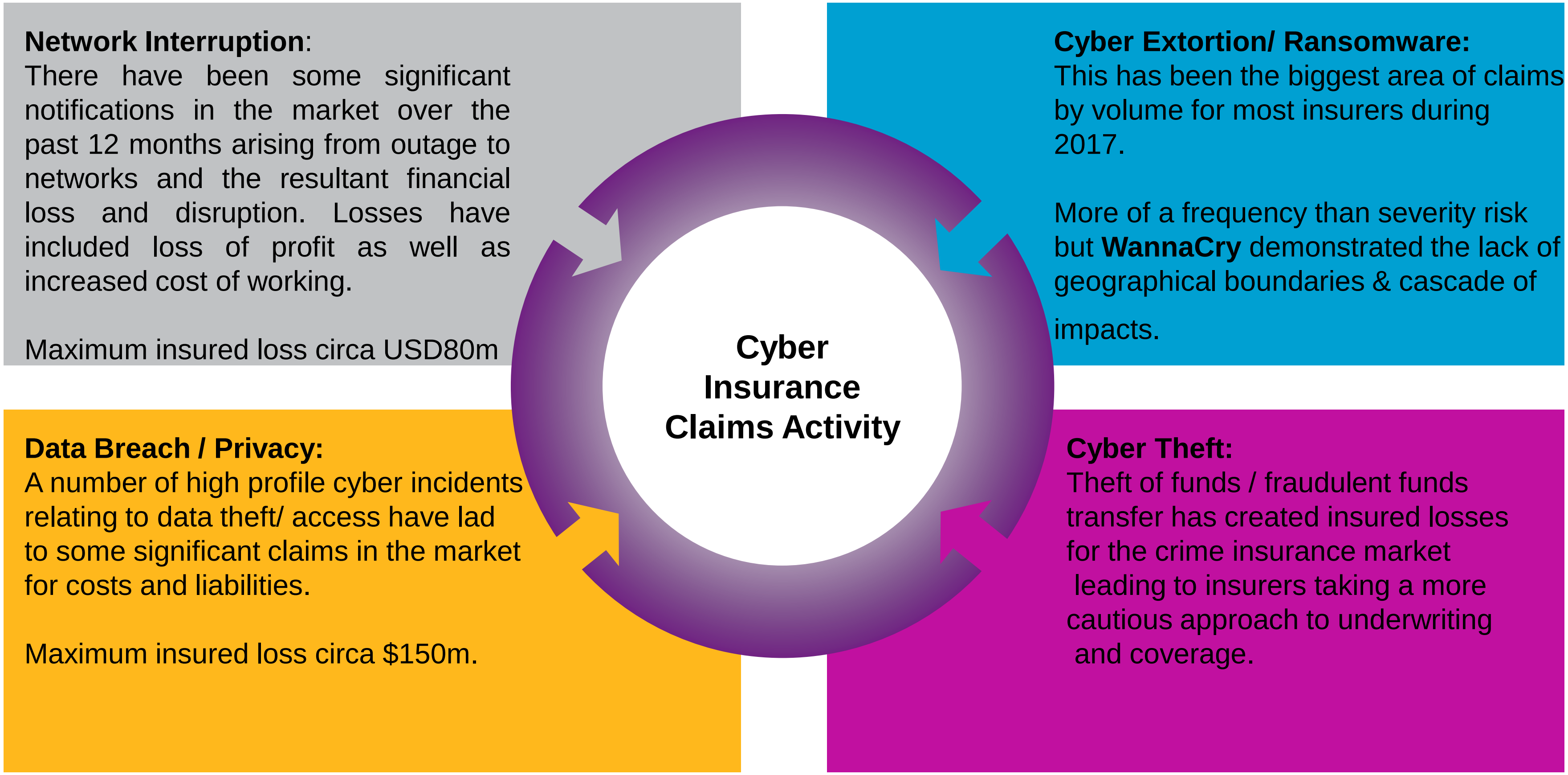
Use the same passwords across all your personal computing devices



(% of 'Yes')

Source: 2017 WTW Cyber Risk Survey, employer survey, UK

Cyber claims activity: What have we seen?



Network Interruption:
There have been some significant notifications in the market over the past 12 months arising from outage to networks and the resultant financial loss and disruption. Losses have included loss of profit as well as increased cost of working.

Maximum insured loss circa USD80m

Cyber Extortion/ Ransomware:
This has been the biggest area of claims by volume for most insurers during 2017.

More of a frequency than severity risk but **WannaCry** demonstrated the lack of geographical boundaries & cascade of impacts.

Cyber Insurance Claims Activity

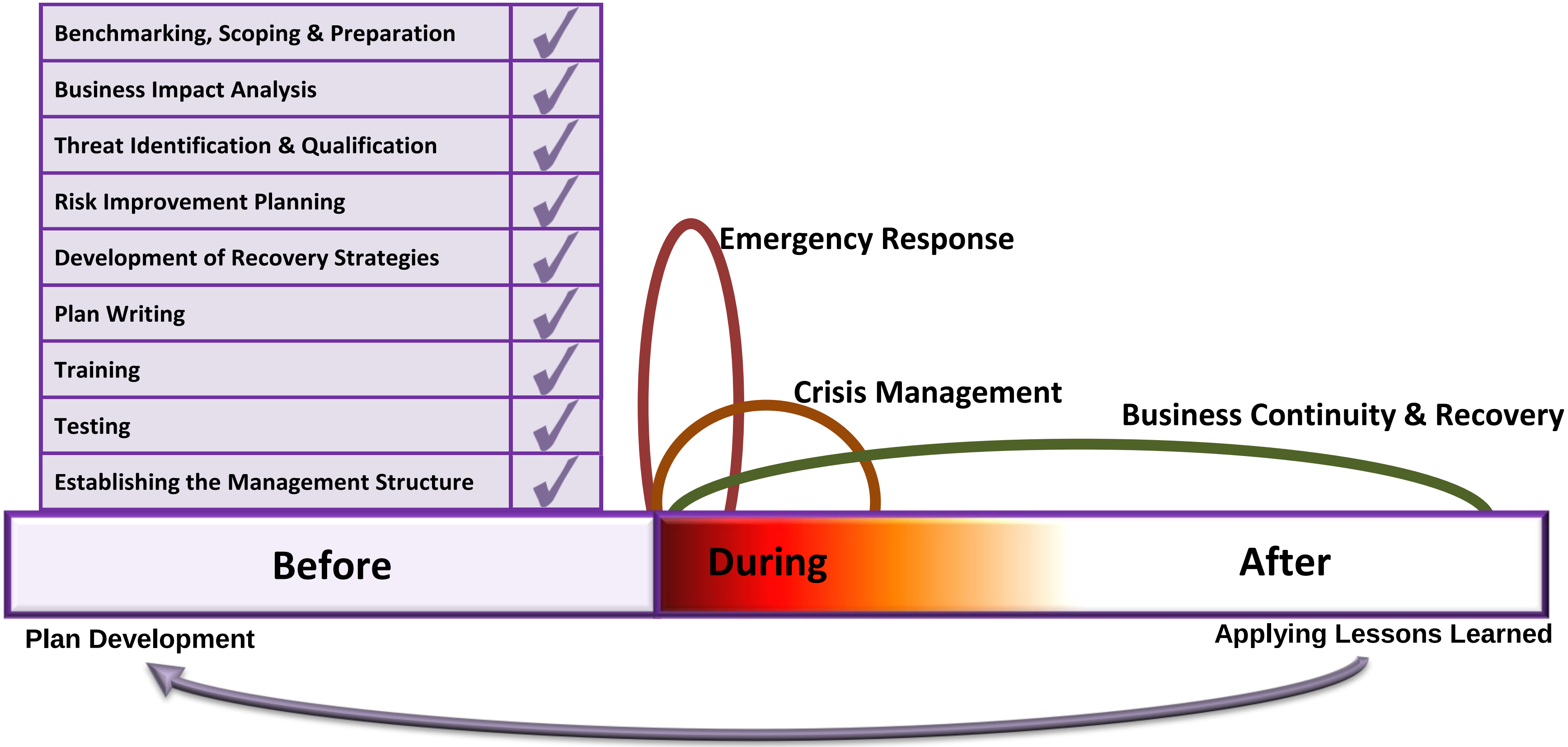
Data Breach / Privacy:
A number of high profile cyber incidents relating to data theft/ access have lad to some significant claims in the market for costs and liabilities.

Maximum insured loss circa $150m.

Cyber Theft:
Theft of funds / fraudulent funds transfer has created insured losses for the crime insurance market leading to insurers taking a more cautious approach to underwriting and coverage.

Cyber event timeline

Technology failure



Benchmarking, Scoping & Preparation	✓
Business Impact Analysis	✓
Threat Identification & Qualification	✓
Risk Improvement Planning	✓
Development of Recovery Strategies	✓
Plan Writing	✓
Training	✓
Testing	✓
Establishing the Management Structure	✓

Handling Cyber Claims - ReSecure

A good Cyber policy will provide a specialist crisis-management response via a 24/7 hotline to help manage the event

A 24 Hour hotline for legal support via

IT Forensics support via and

Credit monitoring, call centres and notifications via Experian

PR and crisis management advice via and

All joined via a live case management system.

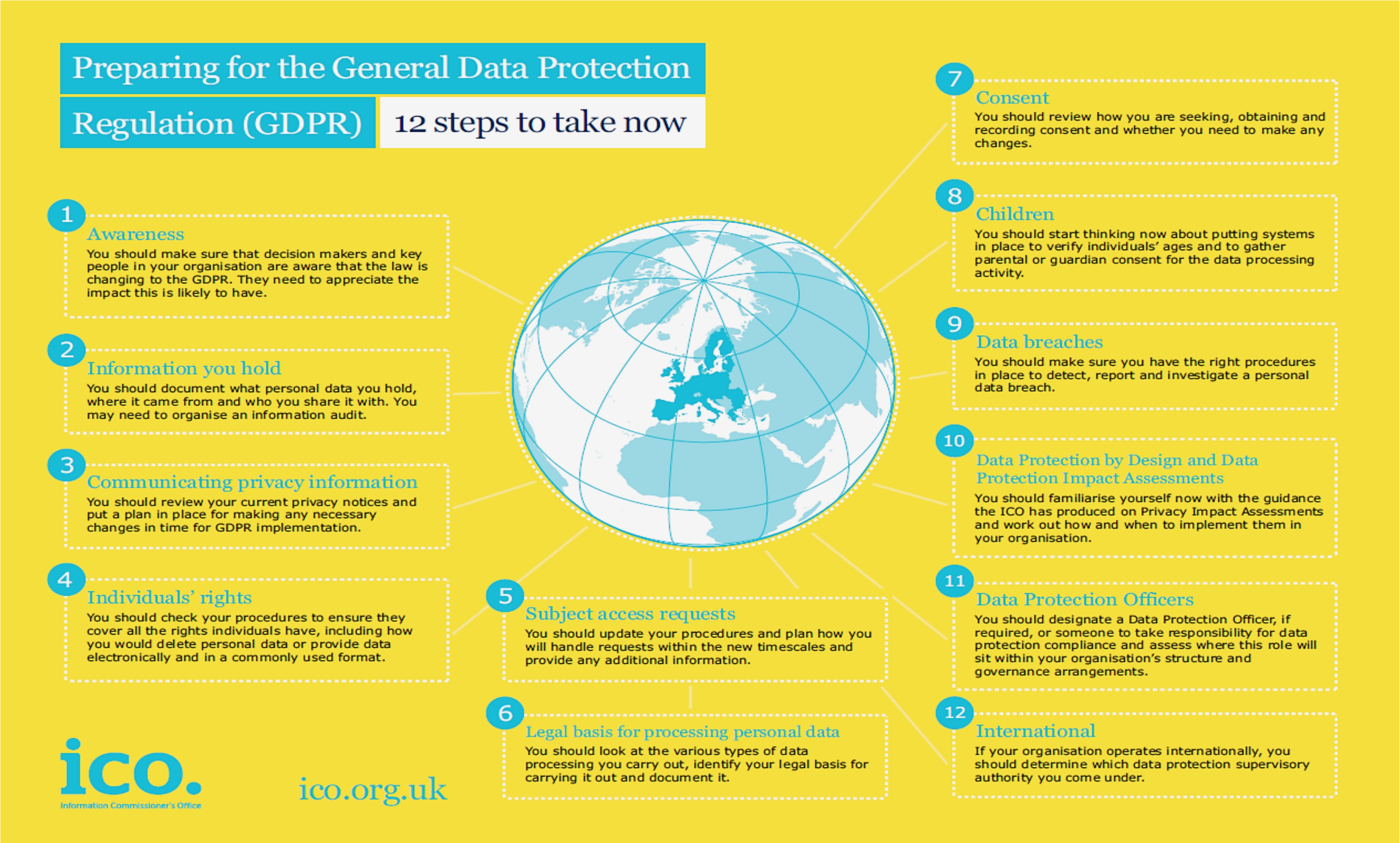
How to talk about Cyber

Mid-Market specific proposition

Questions to Raise during the Meeting:

- ✓ Have you undertaken internal discussions to assess your vulnerability to a cyber attack?
- ✓ Do you think you might be a target? If no, then why?
- ✓ If you do not consider yourself to be a target, could you support that conclusion with evidence ?
- ✓ Where does “cyber risk” appear on your risk register?
- ✓ Have you considered risk management strategies for cyber risk? Is there a report to support this?
- ✓ Have you identified the type of information you hold within your network or “off site” with a cloud provider or data centre?
- ✓ Have you tried to quantify your exposure?
- ✓ Have you considered an exercise to map your exposures into an insurance policy, to identify insurable cyber risks and non-insurable cyber risks?
- ✓ Have you thought about how the changing regulatory environment might effect your business?
- ✓ Information WTW requires to get a VRI
- ✓ The process to get a cyber quote
  - ✓ Proposal form
  - ✓ Conference call
  - ✓ Managing expectation around time it takes to get quotations

General Data Protection Regulations (GDPR)



Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

1 **Awareness**
You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 **Information you hold**
You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 **Communicating privacy information**
You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 **Individuals' rights**
You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 **Subject access requests**
You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 **Legal basis for processing personal data**
You should look at the various types of data processing you carry out, identify your legal basis for carrying it out and document it.

7 **Consent**
You should review how you are seeking, obtaining and recording consent and whether you need to make any changes.

8 **Children**
You should start thinking now about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.

9 **Data breaches**
You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 **Data Protection by Design and Data Protection Impact Assessments**
You should familiarise yourself now with the guidance the ICO has produced on Privacy Impact Assessments and work out how and when to implement them in your organisation.

11 **Data Protection Officers**
You should designate a Data Protection Officer, if required, or someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

12 **International**
If your organisation operates internationally, you should determine which data protection supervisory authority you come under.

ico.
Information Commissioner's Office

ico.org.uk

EU Network & Information Security Directive

Overshadowed by the GDPR?

Before 9 May 2018, you should (if you provide “essential” or “digital” services) put in place

adequate cyber security defences to demonstrate best endeavours in providing continuity of the essential or digital service

Supply Chain Risks

Consider:

1.Are you a subcontractor to someone else. Do you have remote access to their systems? Are they a target to hackers? Are <u>you</u> the weak link?

2.Do you have data that is attractive to hackers? Do you have subcontractors? Do they have remote access to your systems? Are <u>they</u> the weak link?

Subcontractors I.T. security should be a vital part of your vetting process when choosing partners. They may ruin all your good work to be secure, and they or you can cause more liability than you thought you had.

System Failure

Going Beyond Core Cyber Insurance Coverage

any unintentional and unplanned outage of a **Company's Computer System**; or

any negligent act or failure to act by an employee of the **Company**, related to any operating, maintaining or upgrading of a **Company's Computer System**, but excluding any operating, maintaining or upgrading of any cloud service or other hosted computer resources used by the **Company** or any employee "Bring Your Own Device" used to access a **Company's Computer System** or **Data** contained therein.