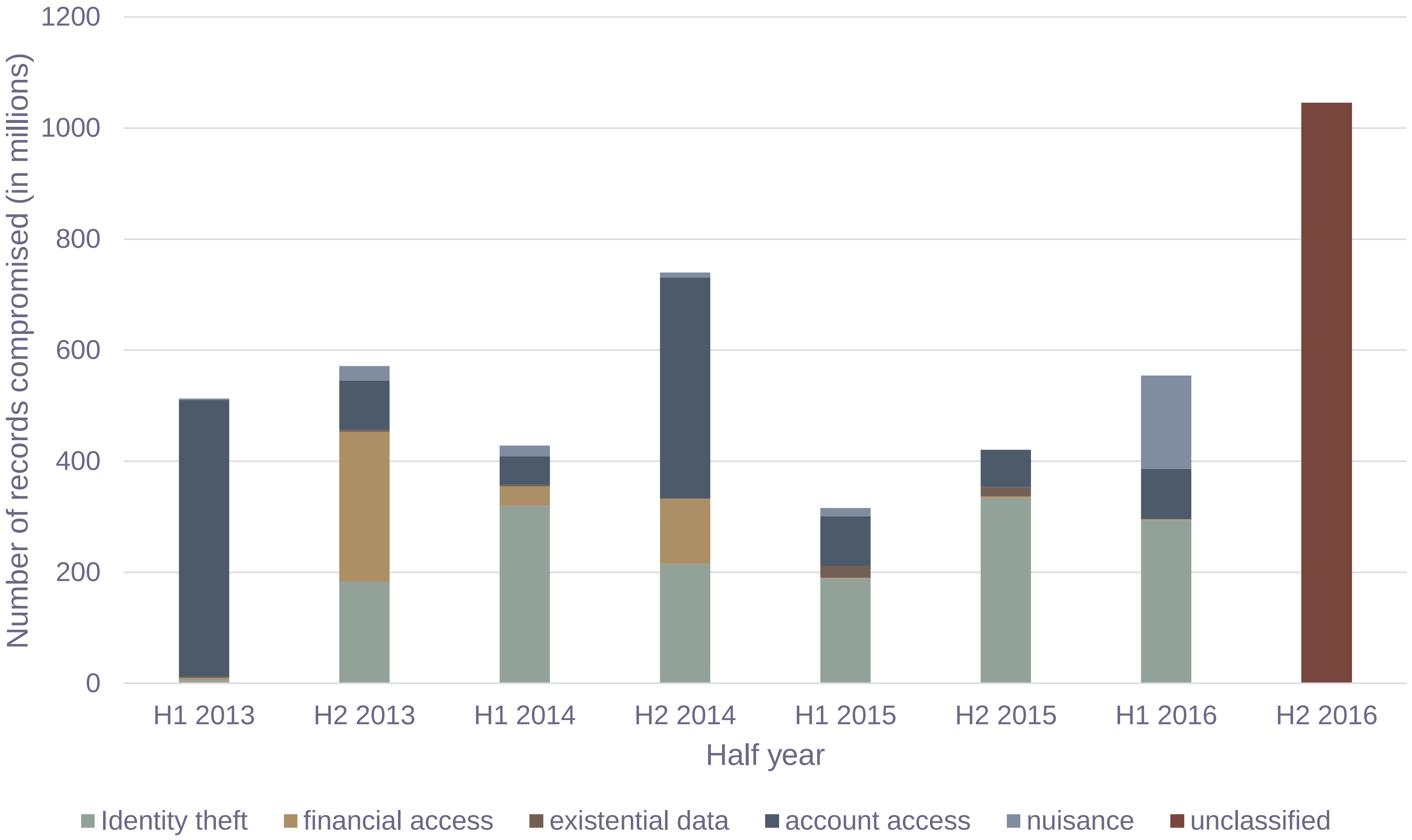
RISK-X ON GDPR

The 12 steps the ICO recommends that you take now

Risk-X
YOUR DATA. ASSURED.

WHY CHANGE THE LEGISLATION?

Data compromises last 4 years



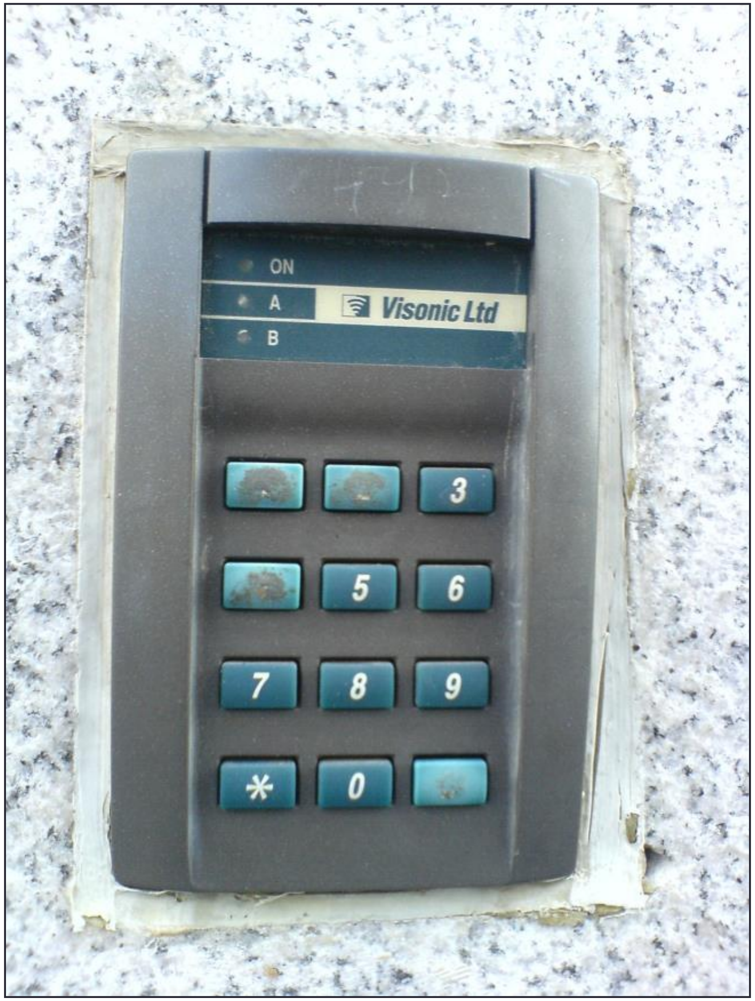
Responses to data loss

- This attack was sophisticated so we were the victim of something that we had no way to protect ourselves against. We could not have foreseen or prevented this attack, but we “take security seriously” so please don’t sue us, stop shopping with us or close your accounts!

- 98% of all breaches that we investigate are UNsophisticated and could have been easily prevented

It really is this simple!

“We have electronic door locks at every entrance, with minimum 4 digit PINs”



“Business seems to need to be incentivised to undertake change by being threatened with a big stick! The only thing that seems to work is significant monetary penalty or executives going to jail. We saw this with PCI DSS and now with GDPR – 4% of global turnover or €20m whichever is greater!

Will it work?”

SO WHAT CAN YOU DO ABOUT IT?

What are the 12 steps the ICO recommends you do now?

The 12 areas to start with are:

- Awareness
- Information you hold
- Communication
- Individual rights
- Subject access requests
- Legal basis for processing
- Consent
- Children
- Data breach
- Protection by design
- Data Protection Officer
- International

Awareness

- GDPR like other requirements only works top down. Start with the board and executives!
- You need their support (time, money, resources)
- Execs need to be aware of the consequences and what it means for them
- Execs need to be signed up and involved, as ultimately they will be accountable
- Then slowly the rest of the organisation needs to be aware

Information you hold

- You will hear lots of information today about the use of technology to find the data that you hold, and this is important – as you are expected to undertake a data audit
  - Remember this now includes hardcopy materials as well if they are indexed
  - It could also include pseudo anonymised data depending on usage
- However, what are the business processes that underpin how you acquire the data?
- How do you process it?
- Who do you share it with and what do they do with it?
  - You can outsource responsibility but not accountability (i.e. liability)
  - If you are the controller then you are still accountable!

Communication

What information must be supplied?	Data obtained directly from data subject	Data not obtained directly from data subject
Identity and contact details of the controller or representative	✓	✓
Purpose of the processing and the legal basis for the processing	✓	✓
The legitimate interests of the controller or third party	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data part of a statutory or contractual requirement	✓	
The existence of automated decision making	✓	✓
When should information be provided?	At the time	Within one month or at time of communication

Individual rights

1. The right to be informed (already discussed in the previous slide)
2. The right of access (will be discussed in the next slide)
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Subject access requests (SAR's)

- In most cases you will not be able to charge for SAR's
  - You can charge a reasonable fee (to cover administrative costs) when a request is unfounded or excessive (particularly if repetitive)
- You will only have a month to respond rather than 40 days
  - You can extend this period by a further two months where requests are complex or numerous
  - But you must inform the individual within one month of the request
- You can refuse a request but you must explain why and that the individual has the right to complain
- You must identify the individual making the request using reasonable means
- If the request is electronic you should respond as such in a common format
- Best practice says you should provide secure self service direct access to an individuals data

Legal basis for processing

- 6(1)(a) – Consent of the data subject
- 6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- 6(1)(c) – Processing is necessary for compliance with a legal obligation
- 6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person
- 6(1)(e) – Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- 6(1)(f) – Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Consent

- Consent under the GDPR requires some form of clear affirmative action. Silence, pre-ticked boxes or inactivity does not constitute consent

- Consent must be verifiable. This means that some form of record must be kept of how and when consent was given and Individuals have a right to withdraw consent at any time.

- Where you already rely on consent that was sought under the DPA or the EC Data Protection Directive (95/46/EC), you will not be required to obtain fresh consent from individuals if the standard of that consent meets the new requirements

Children

- Where services are offered directly to a child, you must ensure that your privacy notice is written in a clear, plain way that a child will understand

- If you offer an ‘information society service’ (i.e. you ask for remuneration, direct marketing or online profiles can be created) directed at children, you will need to obtain consent from a parent or guardian to process the child’s data.

- Children are consider aged 16 and under but the UK has indicated that this may change to 14 to be in line with US legislation

Data breach

- A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

- For example, you will need to notify the relevant supervisory authority about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.

- You also need to notify the individual where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.

- A notifiable breach has to be reported to the relevant supervisory authority within 72 hours of the organisation becoming aware of it, and you can provide information as it becomes available

- If the breach is sufficiently serious to warrant notification to the public, the organisation responsible must do so without undue delay.

Protection by design (and default)

- You have an obligation to implement technical and organisational measures to show you have considered and integrated data protection when processing

- Data protection impact assessments should be used for (at minimum in my opinion):

  - using new technologies

  - the processing is likely to result in a high risk to the rights and freedoms of individuals

- Whether or not the ICO recommends DPIA you should consider using these for all occasions to check if privacy information is impacted

- It really should be as simple as embedding review and risk assessment into project / programme management solutions. Especially as the GDPR promotes governance and accountability

Data Protection Officer

- You must appoint a data protection officer (DPO) if you are a public authority, carry out large scale systematic monitoring or process special categories of data relating to criminal convictions / offences

- NOTE: Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations under the GDPR

Data Protection Officer Cont.

Tasks of the DPO

- To inform and advise the organisation and its employees about their obligations to comply
- To monitor compliance with the GDPR including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed

Employer duties

- The DPO reports to the highest management level of your organisation – i.e. board level
- The DPO operates independently and is not dismissed or penalised for performing their task.
- Adequate resources are provided to enable DPOs to meet their GDPR obligations.

International

- If you operate internationally then which supervisory authority do you fall under?

- The lead authority is determined according to where your organisation has its main administration or where decisions about data processing are made.

- If you are uncertain over which supervisory authority is the lead for your organisation, map out where your organisation makes its most significant decisions about data processing

Summary

Business recommendations

- Use a management framework and align with IT (ISO27001 is a good place to start)
- Make sure that you can demonstrate your compliance as the burden of proof is considerably higher
- Map business processes / know where data is
- Communicate clearly with individuals and generate value to get their data
- Develop and use approved codes of conduct
- Change departmental structures to provide oversight and governance to ensure DPIA
- Conduct 3rd party due diligence and audit
- Have good legal counsel, and get good advice!

IT recommendations

- Align your Information security management framework with the privacy requirements (ISO27001)
- Budget, support and resources will be required to ensure that you do not get compromised
- Have a forensic and incident response contract
- Get basic security right: Asset information, configuration management, patching, anti-virus, encryption, removal of legacy solutions etc.
- Search for data, remove what is not required, anonymise what you can and restrict access to what is left
- Ensure IT strategy aligns with business requirements
- 3rd party technical audit and data controls

Useful Links and information sourced from

- The GDPR
  - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
- Article 29 Working Party updates
  - http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
- ICO overview of the GDPR
  - https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
- ICO 12 steps to take now
  - https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
- Use the ICO’s website as there is fantastic information there

THANK YOU

Any Questions?

Steve Marshall – Managing Partner / Executive Chairman

Professional Experience

Steve is a world class consultant and business executive that has focused on high profile security projects for the government and leading commercial organisations. Steve specialises in compliance, breach clean-up, enterprise architecture validation, assurance, corporate/information security, security restructures and risk in sector leading organisations across many business verticals and markets. A balance of technical excellence and keen business acumen enables Steve to provide cost effective robust strategies for business.

Steve's early career focused on system and network administration / engineering / security on high throughput transactional platforms, video content delivery, high profile websites and hosting infrastructure. Steve then moved into management and senior management within several system integrators and consulting companies. Having developed several practices in the UK and worked for many companies and organisations Steve has now setup PTP Consulting with his partners to provide leading audit, advisory and digital forensics in the UK.

To date Steve has also been involved in :

- High profile security consulting for government organisations
- Headed up and consulted on numerous global retailers PCI DSS compliance programmes
- Provided compliance strategy to several global telecommunication, retail, banking and UK building societies
- Provided architecture validation and security consulting to many enterprise customers
- Provided threat analysis and forensic readiness consulting to many commercial organisations
- Public speaking events themed around security, compliance and IT risk management to audiences in the UK and internationally

Industry Sector Experience

- Financial Services
- Retail
- Media / Leisure / Entertainment
- Telecoms / ISP / Hosting
- Government / Public Sector
- Energy and Utilities
- Transit
- BPO's / Call Centres / Outsourcers
- Gambling and Gaming

Qualifications

- BSc (Hons)
- Qualified Security Assessor (QSA)
- PECB Certified ISO27001:2013 Lead Implementer
- IBITG Certified ISO27001 Lead Auditor
- Professional member of the BCS (MBCS), ISACA & (ISC)^2

About us

- Risk-X is an independent global provider of Audit, Advisory, Forensics, Incident Response, Assurance and Training services.

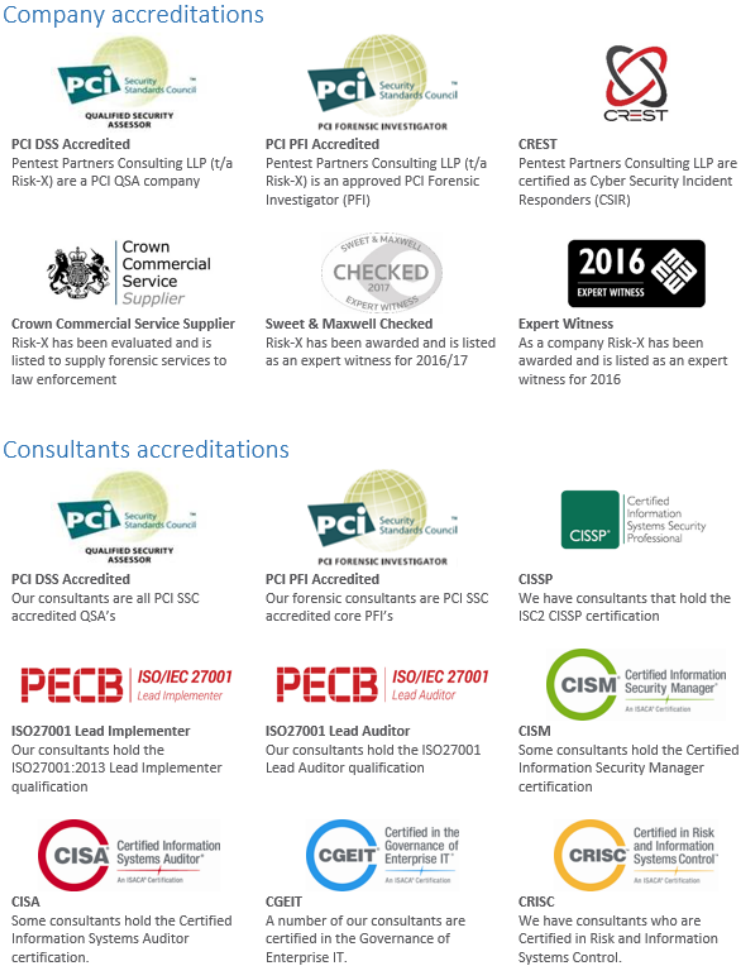
- With over 30 years’ experience, we are a Qualified Security Assessor Company (QSAC) and PCI Forensic Investigator (PFI) in good standing with the Payment Card Industry Security Standards Council (PCI SSC) and are a certified member of the CREST Cyber Security Incident Response (CSIR) scheme through our parent company Pentest Partners Consulting LLP.

- With offices in Cambridgeshire, Bracknell, Cape Town, and Johannesburg we are supported by our secure laboratory facility and globally mobile consulting team.

- Risk-X are specialists in payment, privacy, corporate / information security and dealing with cyber security breaches.

- So whether you are a public or private sector organisation, Risk-X will be able to assist you with all of your corporate governance, regulatory, compliance, audit, advisory, testing and training objectives.

- Steve Marshall
- Executive Chairman
- Steve.marshall@risk-x.co.uk
- +44 7770 352438



Company accreditations

PCI DSS Accredited
Pentest Partners Consulting LLP (t/a Risk-X) are a PCI QSA company

PCI PFI Accredited
Pentest Partners Consulting LLP (t/a Risk-X) is an approved PCI Forensic Investigator (PFI)

CREST
Pentest Partners Consulting LLP are certified as Cyber Security Incident Responders (CSIR)

Crown Commercial Service Supplier
Risk-X has been evaluated and is listed to supply forensic services to law enforcement

Sweet & Maxwell Checked
Risk-X has been awarded and is listed as an expert witness for 2016/17

Expert Witness
As a company Risk-X has been awarded and is listed as an expert witness for 2016

Consultants accreditations

PCI DSS Accredited
Our consultants are all PCI SSC accredited QSA’s

PCI PFI Accredited
Our forensic consultants are PCI SSC accredited core PFI’s

CISSP
We have consultants that hold the ISC2 CISSP certification

ISO27001 Lead Implementer
Our consultants hold the ISO27001:2013 Lead Implementer qualification

ISO27001 Lead Auditor
Our consultants hold the ISO27001 Lead Auditor qualification

CISM
Some consultants hold the Certified Information Security Manager certification

CISA
Some consultants hold the Certified Information Systems Auditor certification.

CGEIT
A number of our consultants are certified in the Governance of Enterprise IT.

CRISC
We have consultants who are Certified in Risk and Information Systems Control.