



*Data Security and Privacy Risks:
Managing these risks in a changing legal and regulatory environment*

Emily Freeman, Executive Director,
Technology & Global Privacy Practice

Major Topics

»» Fundamentals

»» Legal and regulatory environment

»» Financial and Reputational Costs

»» Risk management identification, prevention, mitigation, and transfer thru contracts and insurance -- best practices



FUNDAMENTALS

Security and Privacy Liability

Network and Privacy Liability Risk Basics—People, Processes, and Technology in an Ever-Changing Environment

SECURITY LIABILITY

Was unencrypted computerized information or paper documents containing personally identifiable non-public information (customer or employee) acquired or accessed by an unauthorized person? Is there a potential for financial fraud or identity theft from this breach?

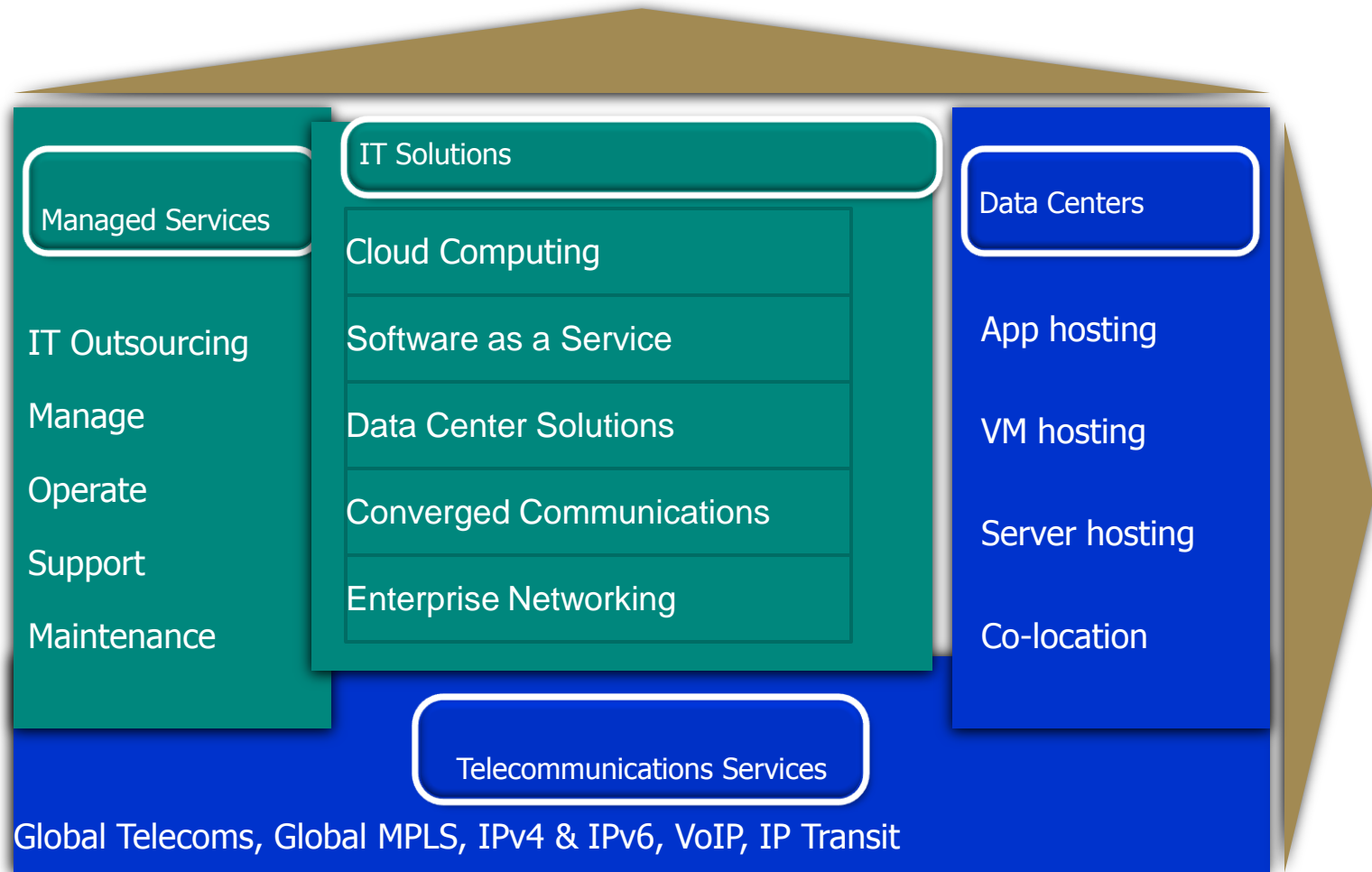
Was sensitive third party corporate information exposed?

PRIVACY LIABILITY

- ❖ Has there been a violation of privacy laws or regulations that permit individuals to control the collection, access, transmission, use, sharing, transfer, and accuracy of their personally identifiable non-public information?
- ❖ EU Data Directive 7 Principles: Notice, Purpose, Consent, Security, Disclosure, Access, and Accountability
- ❖ The difference between promise and performance.

- ❖ What is PII and PHI? Key categories – financial and healthcare
- ❖ Responsibility is on the data controller/owner worldwide to its customers and employees (even if data is transferred to business partner/vendor whether located on/offshore).
- ❖ It's not where you are located, but where the affected persons reside.
- ❖ From nuisance/malicious hacking motives through extortion and terrorism.
- ❖ Identity theft is a business and heavily involves organized crime around the world.
- ❖ Constant evolution of threats and attacks such as social engineering ruses.

Data Protection Risks in a Changing World





LEGAL AND REGULATORY PICTURE

Always changing....

Current status in Europe (i)

- ❖ A “Directive” is a legislative act of the European Union which requires all EU member states to implement laws to achieve a particular result.
- ❖ Key EU Directives – 95/46/EC and e-Privacy Directive 2002/58/EC
- ❖ Expanding interpretation of EU Directive 95/46/EC
 - Art. 17 – Security of Processing
 - ❖ *Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.*
 - ❖ *Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.*
 - Art. 1 – Fundamental rights and freedoms – right to privacy
 - ❖ NB Recital 37 – Security paramount over privacy rights

EU Developments

- ❖ Under the revised EU Directive 2002/58/EC (the “e-Privacy Directive”), which came into force on May 25, 2011, telecommunications firms and internet service providers are already subject to mandatory data breach notification requirements. This Directive’s notification provisions are very similar to many of the existing state notification laws in the United States. For example, the Directive:
 - conditions individual notification requirements on a risk of harm standard;
 - notification must be made “without undue delay”; and
 - the definition of “breach” tracks the language commonly used in U.S. notification laws.
 - While the Directive does not explicitly provide for specific enforcement penalties comparable to the enforcement provisions of U.S. notification laws, many EU member states have instituted fines and penalties for violations of laws enacted under the existing E-Privacy Directive
- ❖ At various forums, senior EU Data Protection officials have signaled their intention to extend that obligation across all business sectors, which, in their view, would help businesses to regain the trust of users of the Internet and online services. Timing?
- ❖ Context of large cross-country data breaches – Epsilon, Sony PlayStation, etc.

Current status in Europe (ii)

- ❖ (Un)favourable interpretation of existing law
 - Cyprus, Czech Republic, Estonia, Sweden
- ❖ Notable legislative amendments:
 - Germany - *Bundesdatenschutzgesetz* (BDSG)
 - Norway - Act of 14 April 2000 No. 31
 - Austria - S. 24 (2a) Austrian Data Protection Act
- ❖ Proponents for new law
 - Ireland – Personal Data Security Breach Code of Practice
 - Netherlands & Finland: “Strong demand for data breach law”
 - UK
- ❖ Encroachment of sectoral legislation
 - Banking - FSA Policy Document, “Data Security in Financial Services”
- ❖ “International” standards
 - BS7799 / ISO 27001 / ISO 27002
- ❖ PCI DSS

UK approach

- ❖ *"Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data"*
 - Guidance from the ICO, 27 March 2008 and 9 February 2010
- ❖ Currently no legal obligation although serious breaches should be reported to the ICO and if appropriate the individual
 - Risk of harm to individuals
 - Volume of data involved
- ❖ Action depends on seriousness of breach
 - Many dealt with informally
 - Q1 2010 – c. 5% of breaches have led to regulatory action (e.g. formal undertakings)
 - Since 2007 – over 1000 breaches have been notified to the ICO

And lastly....

Payment Card Industry - Data Security Standard

- ❖ PCI DSS (October 2010 – Version 2.0; current version V.1.2)
- ❖ Developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., to help facilitate the broad adoption of consistent data security measures on a global basis.
- ❖ PCI applies to ALL organizations or merchants, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data. Said another way, if any customer of that organization ever pays the merchant directly using a credit card or debit card, then the PCI DSS requirements apply.
- ❖ Compliance requirements depend on transaction volume (assignment of levels).
- ❖ Levels dictate whether a self-assessment/scan or outside annual audit by an approved Qualified Service Assessor is required.
- ❖ Exposure – fines and penalties; ultimately loss of privilege; ground for legal action in US



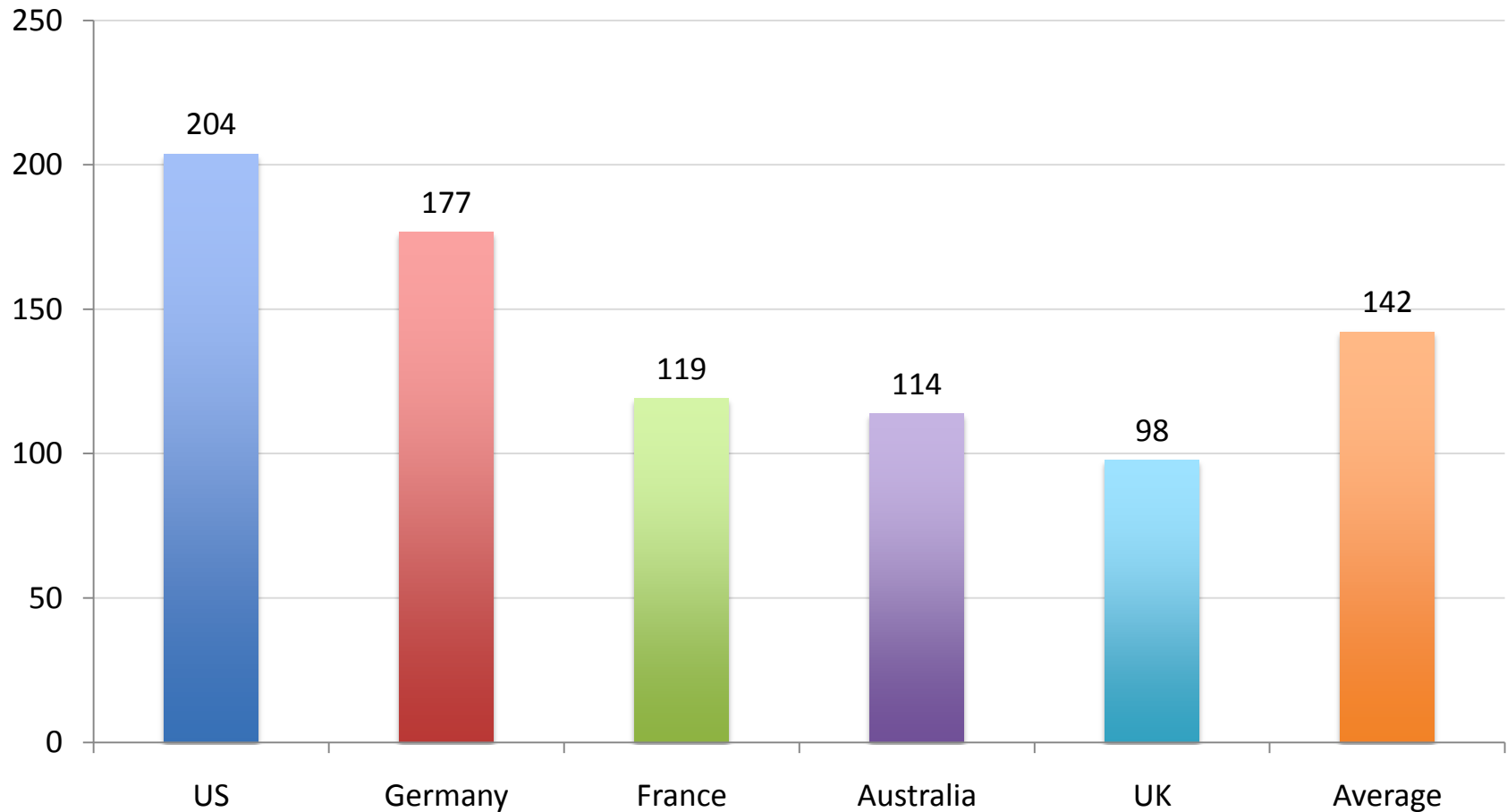
FINANCIAL AND REPUTATIONAL COSTS

Trends and differences

Per capita cost

Converted to \$US dollars

Per capita cost is defined as average cost divided by the number of records lost or compromised



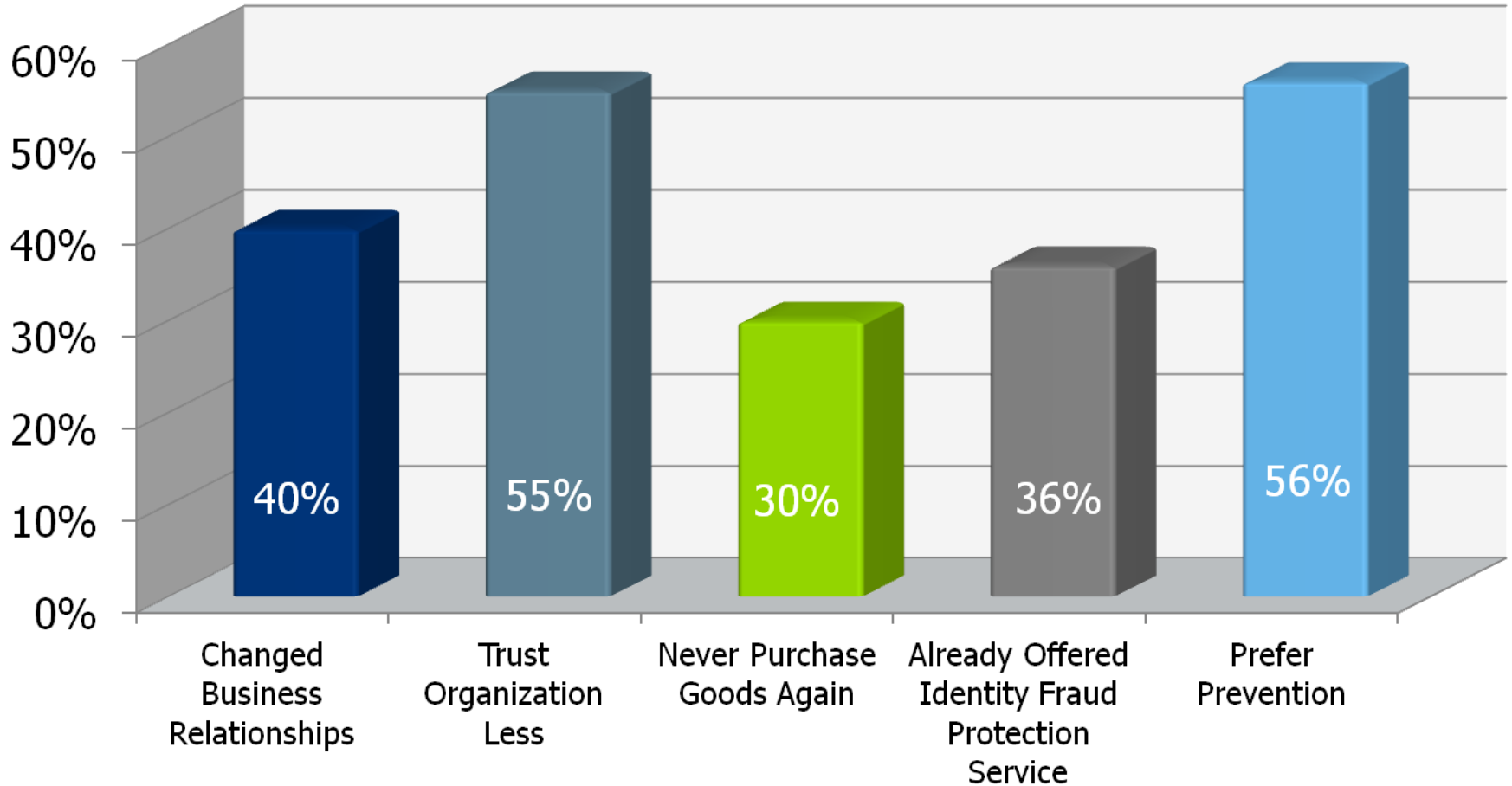
Direct Loss of Data Breaches—U.K. Voluntary Notification

- ❖ Costs reflect voluntary notification; regulatory exposure
- ❖ Average organizational costs - £1.68M.

DATA BREACHES CONTINUE TO BE A VERY COSTLY EVENT FOR ORGANIZATIONS
(Ponemon 2009 Annual Study of a Data Breach)

Cost	2007	2008	2009
Detection & Escalation	£15	£11	£12
Notification	£1	£3	£7
Response	£15	£14	£17
Lost Business	£17	£32	£29
Total	£48	£60	£65

Impact on Brand



Source: Javelin Research Survey, Customer Survey on Data Breach Notification, Javelin Research & Strategy



RISK MANAGEMENT AND INSURANCE

Best practices discussion

Cross Functional Risk Team

- ❖ Redesigning a key corporate function requires senior management buy-in and support from a cross-functional team
- ❖ On-going and empowered
- ❖ Technology, people, and processes focus
- ❖ Compliance and cost/benefit orientation
- ❖ Best practices oriented - Standards and Tools
- ❖ Part of selection process/"go live" decision
- ❖ Key stakeholders:
 - Risk Management
 - Procurement
 - Corporate Legal
 - Business group owners/operational units
 - IT/IS
 - Internal audit/compliance
 - Potentially HR

Best Practices Ideas

- Eliminate unnecessary data; keep tabs on what's left
- Establish an effective vendor risk management strategy where PII/PHI is involved (due diligence, contractual indemnity/other contractual protections and insurance requirements)
- Build security into software development and maintenance from the start
- Regularly test and review web applications
- Compliance/audits at regular intervals and as required (pen testing/scans/process)
- Audit user accounts and monitor privileged activity
- Filter outbound traffic; data leakage prevention program
- Encrypt PII/PHI at rest, in transit and on mobile devices
- Control mobile devices, USB sticks and tapes
- Security awareness and training
- Role based access/improved access controls
- Monitor and mine event logs
- Patch and incident management
- Develop a cross-border breach notification response strategy that complies with each country's mandates on notifying both employees and government data agencies

What sensitive or confidential information is accessed?

Confidentiality means the information is protected from unauthorized or accidental disclosure, use or theft.

Low: Data which has been explicitly approved for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be freely disseminated without potential harm. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact the company, employees, customers, or other third parties.

Medium: Information that is intended for use within the company. Its unauthorized disclosure could seriously and adversely impact the company, employees, customers, or other third parties. This classification applies to information that requires special precautions to assure the integrity (modification/deletion) of the information.

High: This classification applies to the most restricted business data that is highly confidential or subject to regulatory/civil protection --- customer or employee PII/PHI .

Outsourcing – Potential Risks

- ❖ Vendor may not execute or over-promise.
- ❖ Vendor may not manage customer and project scope.
- ❖ Vendor may not document and communicate effectively.
- ❖ Vendor may not protect their network and yours/others data with the same level of care as you.
- ❖ Vendor may have a malicious or criminal inside employee with highly trusted access.
- ❖ Vendor may suffer financial problems, even bankruptcy.
- ❖ Vendor may be unable to perform because of an unexpected *force majeure* peril, such as political risk, terrorism, or natural disaster.
- ❖ Vendor may use IP to enter into direct competition.
- ❖ Vendor's employees may not keep source code in escrow.
- ❖ Vendor may violate regulations or statutes that apply to their operations – collections, data transfers, privacy, etc.

Vendor Selection and Risk Classification

- ❖ Risk Matrix and “data classification model”
- ❖ High, medium, and low risk definitions
- ❖ New vendors and renewal of existing vendors
- ❖ Due Diligence, contracts and insurance



RISK TRANSFER – CONTRACTS AND INSURANCE

Important Contractual Developments – Service Providers, Business Associates, and Vendors

- ❖ **Beyond negligence to strict liability**
- ❖ **Expanded Contractual Indemnity Provisions** – all aspects of data breaches (civil claims, regulatory investigations and notification costs) – from clients and sponsoring banks
- ❖ **Due diligence and security requirements** – more detailed in contracts including triage/reporting of potential breaches
- ❖ **Insurance requirements** – specific requirements for professional/cyber insurance

Why should you transfer data protection risks through your own insurance program?

- ❖ Many functions are conducted by outside vendors and contractors who may lack insurance and assets to respond. What if the vendor makes a systemic mistake? What if they fail to purchase insurance or keep it? What if they are located in a country where this insurance cannot be obtained? What if the policy they purchased denies coverage or has inadequate limits?
- ❖ PCI (which is the credit card industry security standards) compliant companies have had their security compromised from processes lapse, human error, or criminal insider.
- ❖ No system can be designed to eliminate the potential for loss, as people and processes failures cannot be eliminated. Insiders may be perpetrators.
- ❖ Responsibility rests with the data owner from a legal, regulatory perspective, and credit card association operating regulations.
- ❖ Investor fallout from uncovered losses with large claim and class action potential and major impact on brand and reputation.
- ❖ Traditional insurance does not cover security liability or adequately cover privacy risks – we provide gap analysis assistance to support this conclusion.

Network and Privacy Insurance

- ❖ There is no common insurance language – each underwriter offers a different base product. Manuscript language very important to meet client needs to address risks and contractual exposures.
- ❖ Focus on the quality of the coverage, experience of the underwriter, approach to managing claims, and insurance limits for severity exposure.
- ❖ Cyber Liability capacity - £100 ML +
First Party capacity - £ 50 ML +

Cyber Liability Coverages

❖ Civil Liability

- Defense Costs
- Single/class action
- Potential plaintiffs can include affected data subjects, financial institutions, etc.
- Contractual indemnities to customers (including notification costs)

❖ Privacy/Security Regulatory Actions (aggregate sublimit)

- Defence Costs
- Payment of civil fine or penalty
- Regulatory compensatory award
- PCI Fines (smaller sublimit)

❖ Notification and Crisis Management Costs (aggregate sublimit) – Voluntary, Legally Required, Contractual

- Mailing and tracking costs; Offers of services to affected data subjects, including credit reports, credit monitoring, credit protection, identity theft insurance, etc.; Computer forensics services from outside experts; Outside PR and crisis management support; Legal advice; Professional call center

Lockton Technology and Global Privacy Risk Team

- ❖ Co-leaders: emily.freeman@uk.lockton.com and ben.beeson@uk.lockton.com
- ❖ 5 member core team is comprised of technology and global privacy professionals in London with 10+ years of specialized cyber experience, plus 2 U.S. based specialists.
- ❖ Risk management services to include:
 - Incident Breach Response Plan
 - Vendor Risk Management Program
- ❖ Customized insurance solutions include:
 - Technology and telecom errors and omissions
 - Multimedia Liability
 - Intellectual property infringement including patents
 - First party coverage for data, programs, and networks
 - Data Protection Liability (Security and Privacy Liability)
 - Reputational Harm