PEOPLE I PROPERTY I REPUTATION

ASSET PROTECTION

OK, NOW I BELIEVE!

The Reality of Cyber Risk and Insurance Solutions

March 16, 2016

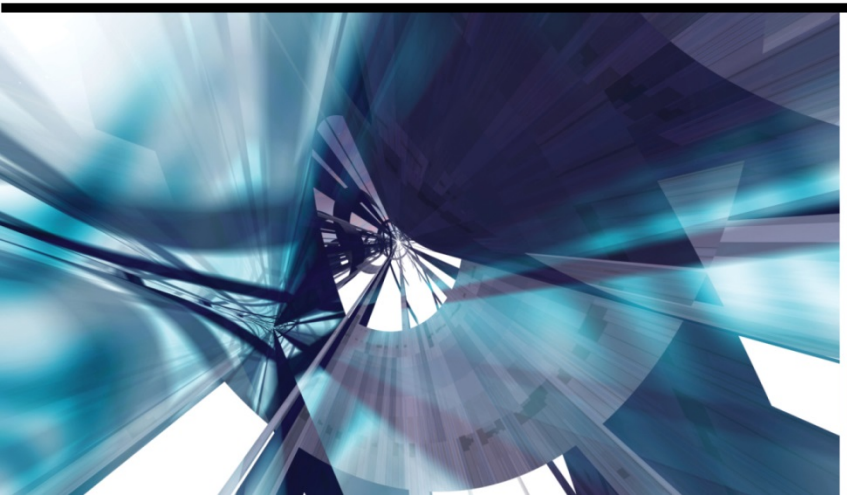
FMI

THE VOICE OF FOOD RETAIL

TABLE OF CONTENTS

PEOPLE I PROPERTY I REPUTATION

CYBER INSURANCE MARKET OVERVIEW



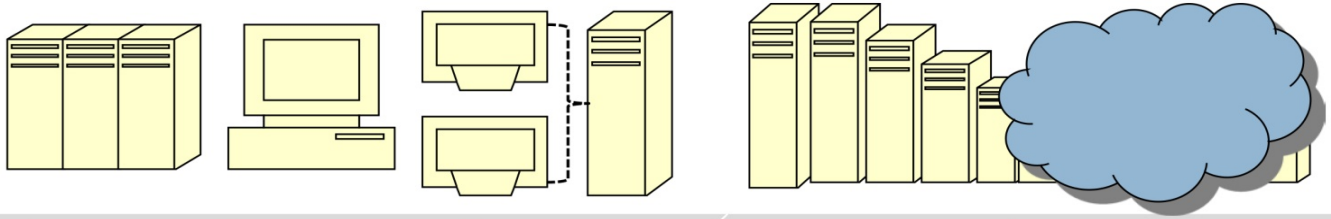
FMI

THE VOICE OF FOOD RETAIL

THE TECHNOLOGY BLUR

------1950s--------1974-----1995----------2005----------2010----------Today--

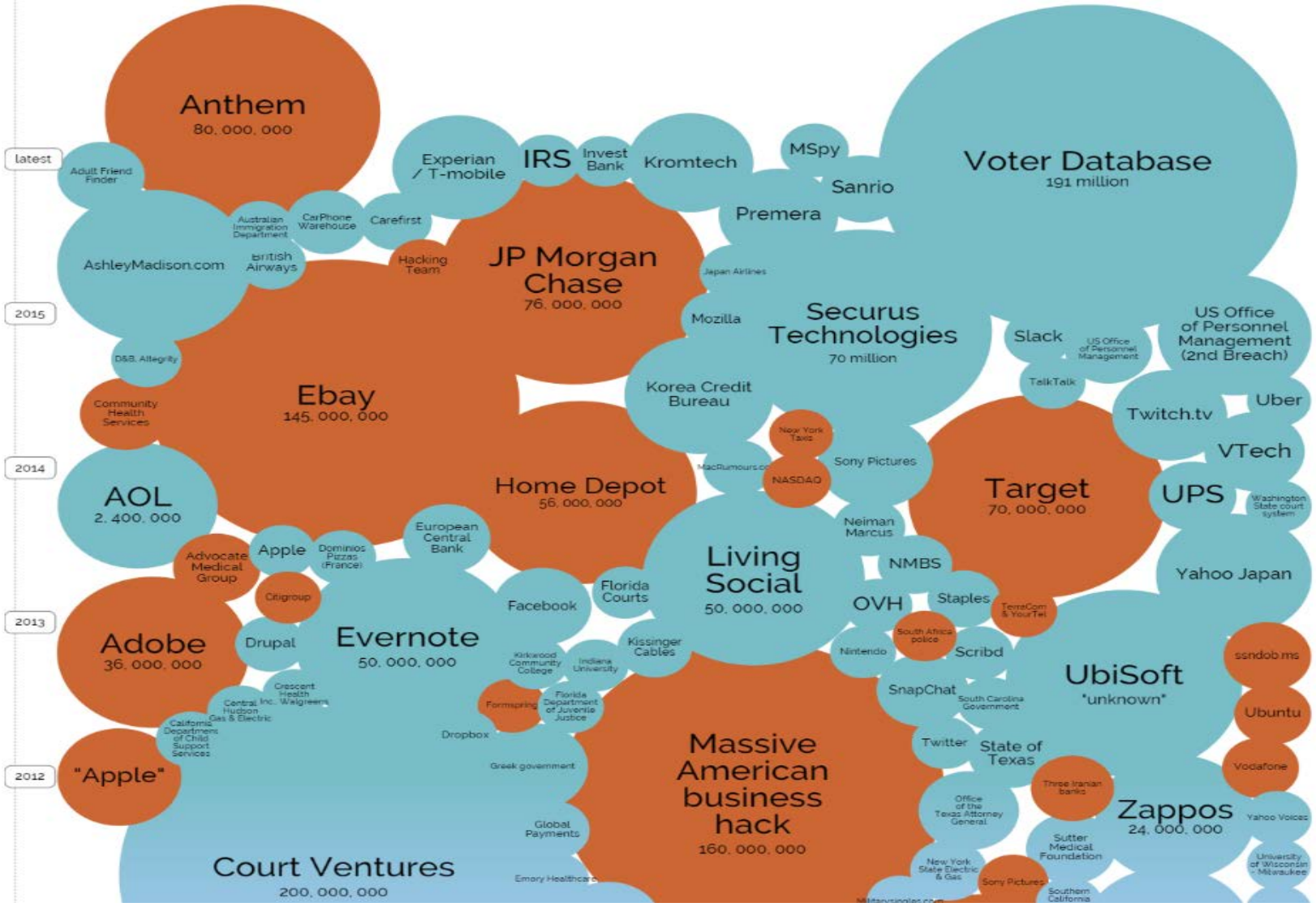
PERIOD OF HISTORICAL CHANGE FOR THE TECHNOLOGY STACK



Technology eras and interfaces of change	Mainframe computing	Mini Computer	Client-server internet	Virtualized data centers	Cloud Solutions
Velocity of change	Multiple decades	About 15 years	About 10 years	Less than 5 years	Quarters and months
Technological	Hybrid circuits catalyst	Integrated circuits	Microprocessor: network and productivity software	Hypervisor and cost-efficient server chips	Mobility, cloud computing and big data
Impact on the technology stack	Birth of hardware, software and services paradigm	Beginnings of distributed architecture; smaller, more accessible	Expansion of distributed architecture and requirements	Conscious decoupling with moderate benefits	Convergence, disruption and new paradigm
Estimate of global value of technology	Much less than US $100 billion	Over US $100	Over US $1.5 trillion	Over US $2 trillion	Over US $3.5 trillion
Technology incumbents (S&P 500)	Under 10	About 40	About 80	About 80	About 70

Source: EY analysis

CYBER MARKET OVERVIEW: LARGEST BREACHES



Source: www.informationisbeautiful.net

CYBER INSURANCE MARKET DEVELOPMENTS

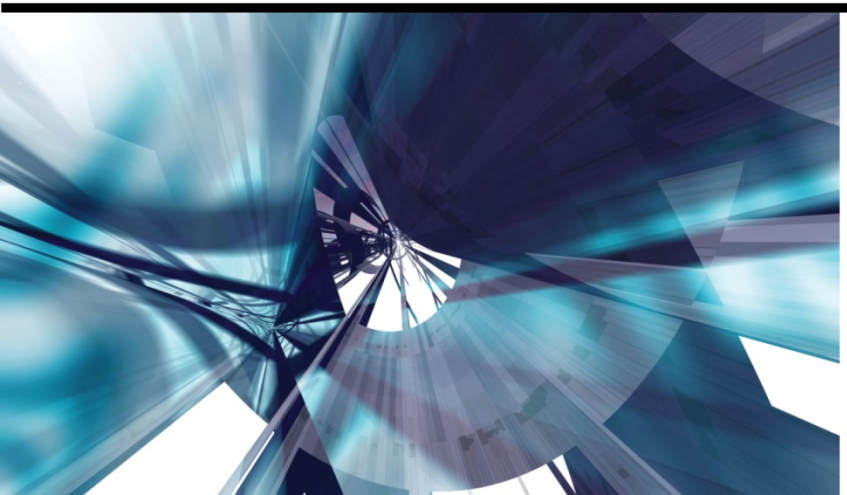
- The cyber insurance market has hardened for the retail/hospitality and healthcare sectors following major breach events to “bulk data collectors” in the last 18 to 24 months. Expect more detailed underwriting requirements and tightening capacity for higher risk industries.
- End-to-End encryption is now required for many retailers and, in some cases, a signed warranty affirming that all systems have been tested/scrubbed for BlackPOS or any similar malware; some underwriters expecting P2PE plan in addition to EMV implementation.
- Mobile device encryption and data tokenization is now a focus for many underwriters.
- Carriers are now strongly aware of the one sided nature of the Merchant Service Agreements and have seen first hand the severity and lack of “due process” involved in calculating PCI fines, penalties and assessments. Litigation between merchants, their processors/acquiring banks and with their insurer(s) is becoming more common.
- Some markets may attempt to reintroduce sub-limits for forensics, notification, credit monitoring and business interruption as a means of controlling their overall exposure

Rank	Sector	Number of Identities Exposed	Percentage of Identities Exposed (100%)
1	Retail	205,446,276	59%
2	Financial	79,465,597	23%
3	Computer Software	35,068,405	10%
4	Healthcare	7,230,517	2%
5	Gov. & Public Sector	7,127,263	2%
6	Social Networking	4,600,000	1%
7	Telecom	2,124,021	.6%
8	Hospitality	1,818,600	.5%
9	Education	1,359,190	.4%
10	Arts and Media	1,082,690	.3%

Top 10 Sectors Breached by Number of Identities Exposed
Source: Symantec

PEOPLE I PROPERTY I REPUTATION

COVERAGE GAPS/INSURANCE SOLUTIONS



FMI

THE VOICE OF FOOD RETAIL

POTENTIAL COVERAGE GAPS IN TRADITIONAL INSURANCE POLICIES

- General Liability policies cover third party loss where there is an unintentional or unexpected loss and are triggered by claims for bodily injury or property damage; also, they generally exclude intentional acts *(Note 2014 ISO General Liability language which excludes cover for data breach costs)*
- Property policies cover damage to property arising out of a direct physical loss and extra expense associated therewith (potentially Business Interruption), but loss must arise from Direct Loss to Tangible Property
- Crime Insurance covers loss to money, securities and other property ("data" is not tangible property)
- Consider D&O implications stemming from cyber security expectations (SEC guidance) and "diligent efforts" to obtain a mechanism to transfer the specific risk

GAPS:

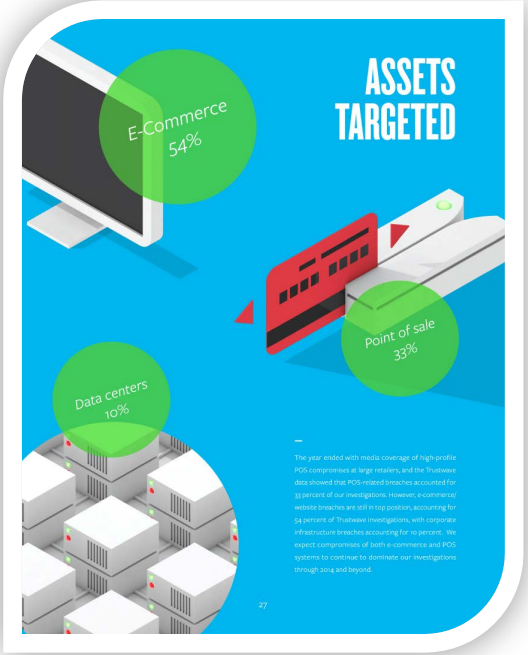
- No coverage for regulatory or card-brand investigations or resulting fines/penalties (PCI-DSS, FCC, FTC, SEC)
- No coverage for theft/destruction of information assets (data, R&D, Trade Secrets, other IP)
- No coverage for loss of use of systems from cyber attack (DDoS, malware, etc.)
- No Extra Expense coverage for hiring forensics and legal teams or costs associated with notification, credit monitoring and other remedial services following a security/privacy breach
- No coverage for economic harm/loss to third parties resulting from a cyber-related event

PRIVACY LIABILITY & INFORMATION SECURITY – EXPOSURES & INSURANCE COVERAGE

TRADITIONAL & NON-TRADITIONAL PRIVACY LIABILITY & INFOSEC RISKS

First Party Risks and Coverage

- Business interruption and extra expense as a result of network or web site outage
- BI/EE for loss of data, recreation of data, uncollectible accounts receivable, corrupted IP
- Cyber extortion – ransomware and/or threats to post/sell security vulnerabilities and/or confidential data
- Theft or destruction of Trade Secrets or other IP

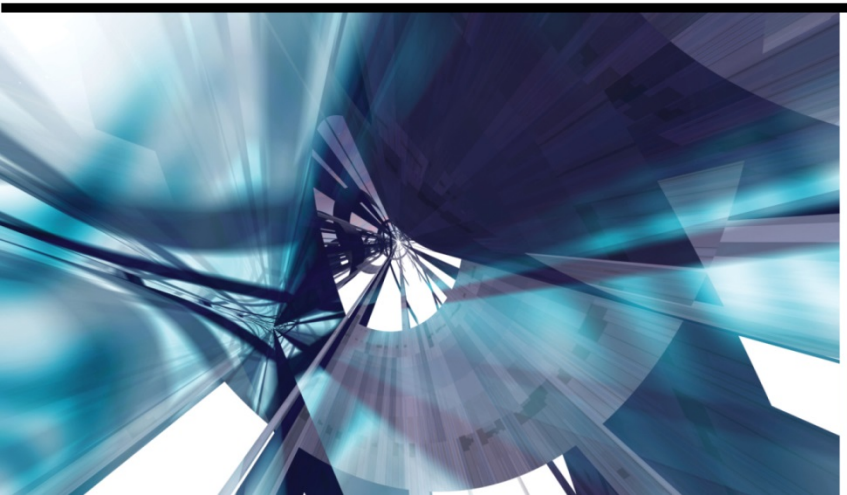


Third Party Risks and Coverage

- Breach notification and mitigation
- PCI Fines, Penalties & Assessments
- Enterprise wide data privacy wrongful acts from either internal “rogue employees” or external “hacker”
- Records wrongfully disclosed whether in electronic or physical format
- Use of your Network to launch an attack or “leapfrog” into third party networks
- Media liability and intellectual property infringement
- Economic harm to your customers due to “down time” of your own application, network, web site upon which your customers rely

PEOPLE I PROPERTY I REPUTATION

LOSS POTENTIAL



FMI®

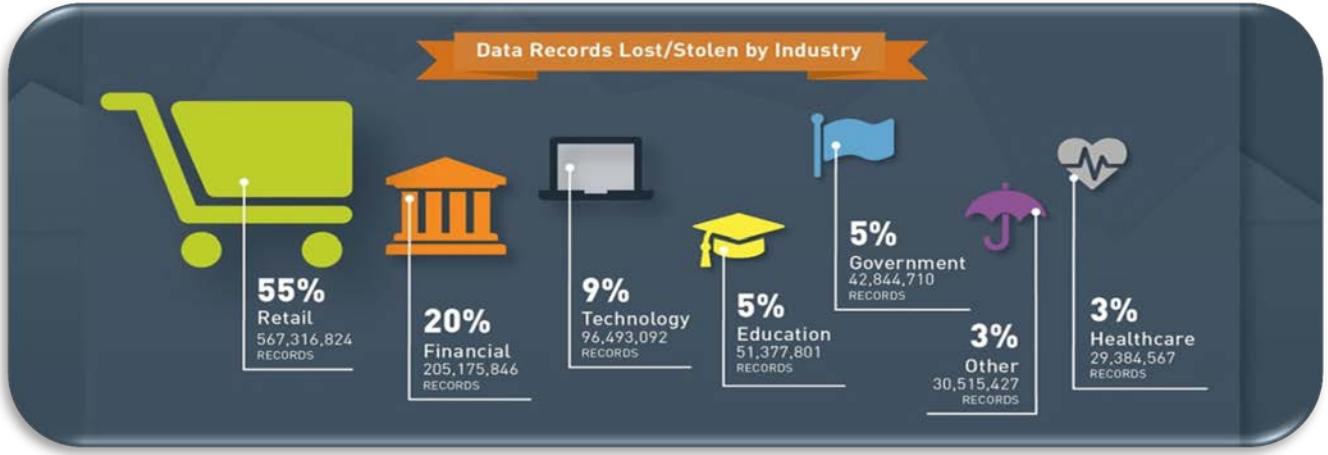
THE VOICE OF FOOD RETAIL

PRIMARY EXPOSURES FOR RETAIL

Logical focus should most likely be upon Data Privacy exposure, including:

- Point-of-sale (POS) transactions
- Cardholder not present transactions (new home delivery concepts)
- Bonus card program details/ customer preferences
- Healthcare information (from pharmacy)
- Personal data of employees (retirees), dependents and beneficiaries

Considerable additional exposure is present in Outsourcing arrangements with various vendors, including H.R./Benefits, Operations (e.g. Target's HVAC vendor Fazio Mechanical) and others. Finally, a network outage could have a significant impact on a company's income and reputation.



CYBER LOSS POTENTIAL

Data Privacy Breach

Company experiences a data privacy breach due to penetration of its network by a hacker, by the unintentional release of non-public info, by the loss/theft of a laptop, or even by loss/theft of legacy hard copy files stored offsite. The breach exposes the personally identifiable information and protected health information (PII and PHI) of customers, employees, vendors and/or business partners. Consider types of data that might be wrongfully accessed/stolen: PII and PHI includes customer names along with social security numbers, DL numbers, credit card numbers, email addresses, phone numbers and/or employee health information (diagnosis, prescription details, treatment plans).

As a result, Company incurs significant losses in order to comply with state/federal privacy laws, regulatory investigations, and defend against consumer class action suits. Cyber policies can be written to respond by providing the following coverage (not provided under current P&C policies):

- Costs to **notify** each person whose data was breached. Also, costs to supply **credit monitoring and ID theft restoration** services as well as set up a **call center** to respond to victim inquiries
- **Legal, public relations and forensic** expenses related to investigating/mitigating the event
- **Regulatory investigations** of the breach by State AGs, FTC and other regulatory authorities (may include **fines, penalties** and **consumer redress funds**)
- Costs associated with **PCI investigation** (mandatory **PFI** is paid for by the merchant); plus **fines** for PCI non-compliance, as well as **assessment charges** (reissuance costs, fraud charges pursuant to MSA)
- **Defense costs and damages** from employee or consumer suits and class actions

CYBER LOSS POTENTIAL

Network Attack

Company's network is penetrated via a spear-phishing campaign which successfully targets key personnel with access. Access is gained when a company employee mistakenly opens a link in an email which appears to be from a manager – with access to the Company's network, the malware uploaded is able to gain control of key servers, passwords, customer data and billing information.

As a result, significant losses are incurred before the attack is detected, neutralized and the network is restarted to bring critical systems back online. Cyber policies can provide the following coverage (not provided in P&C policies):

- **Forensic expenses** to isolate and contain the intrusion, image the compromised servers, and investigate any cascading effects of the attack
- **Extra Expenses** to avoid or minimize the duration of the interruption, including costs to rent equipment or move to a substitute facility (hot site); costs to preserve evidence and costs to substantiate the income loss
- **Loss of Income** due to inability to conduct transactions, order stock, fulfill orders, etc…
- **Fixed operating expenses** (including ordinary payroll) for service which are redundant because of the suspension or deterioration of the insured's business

CYBER LOSS POTENTIAL

Outsourcing

The Hidden Risks of Outsourcing

- Retail companies outsource many functions, including IT and/or data management functions to third party vendors. Consider the evolving challenges associated with:
  - Point of Sale transactions / credit card processing
  - Cloud storage and services
  - Remote monitoring of control systems
  - Back office functions
  - HR and benefits administration
- Outsourcing a function = Loss of Control, but does **NOT** release the "data owner" from liability for privacy violations
- Vendor risk is a function of Statement of Work and Access, not a function of size of contract or size of vendor
- Contract provisions often limit vendor liability (consequential damage waiver, limitations of liability, force majeure, limited indemnity provisions, etc.)
- Regulatory compliance rests with data owner as the front end connection with the customer

CYBER LOSS QUANTIFICATION

Data Breach Loss – 1,000,000 records

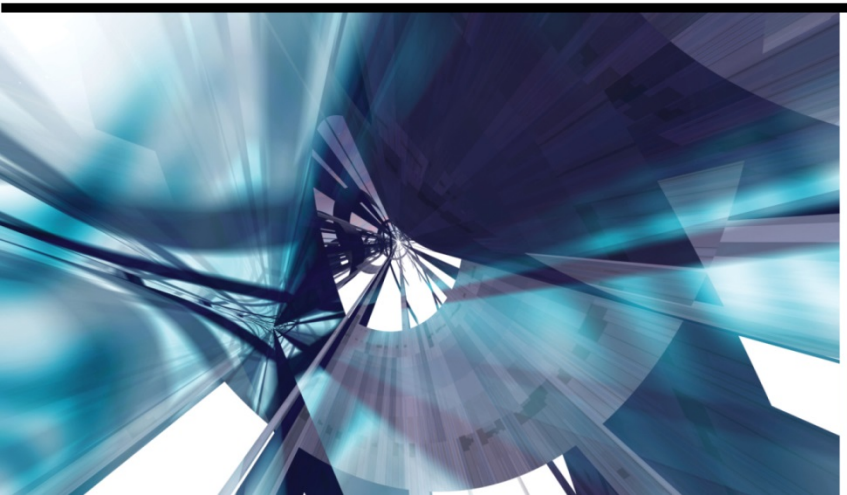
Total Number of Affected Records?	1,000,000
Type of Data Breach?	PHI / PII
Organization's first breach?	Yes
Data is in a centralized system/location?	Yes
Is fraud expected?	Yes
Is PCI compliance an issue?	Possibly
Class Action lawsuit expected?	Yes
Incident Investigation	
Forensics Investigation	$154,000
Security Remediation	$210,000
Data Breach Law Guidance	$38,000
Sub-Total	$402,000
Customer Notification/Crisis Management	
Customer Notification	$1,000,000
Call Center	$75,000
Credit/ID Monitoring	$290,000
Public Relations	$35,000
Sub-Total	$1,400,000

Regulatory and Industry Fines/Penalties/Sanctions	
PCI Fines & Penalties	$50,000
Card Fraud Assessments / Reissuance	$14,500,000
State AG	$635,375
HHS, FTC, SEC, other	$1,428,125
Sub-Total	$16,613,500
Class Action Lawsuit	
Defense	$699,000
eDiscovery	$770,000
Public Relations (add'l.)	$698,750
Sub-Total	$2,167,750
Estimated Totals	
Total Cost	**$20,583,250**
Per Record Cost	**$21**

This illustration represents a conservative estimate of the costs associated with a data breach of 1,000,000 records. The potential exposure of a company to even a minor breach is significant, especially when considering some sources estimate the cost per record breached much higher.

***The numbers presented in the NetDiligence data breach cost calculator are estimates and provided for education and illustration purposes only. Numerical results are based on a proprietary formula developed by NetDiligence and its insurance industry partners. This calculator is not intended to predict insurable perils or related costs.**

AVOIDING THE LAND MINES

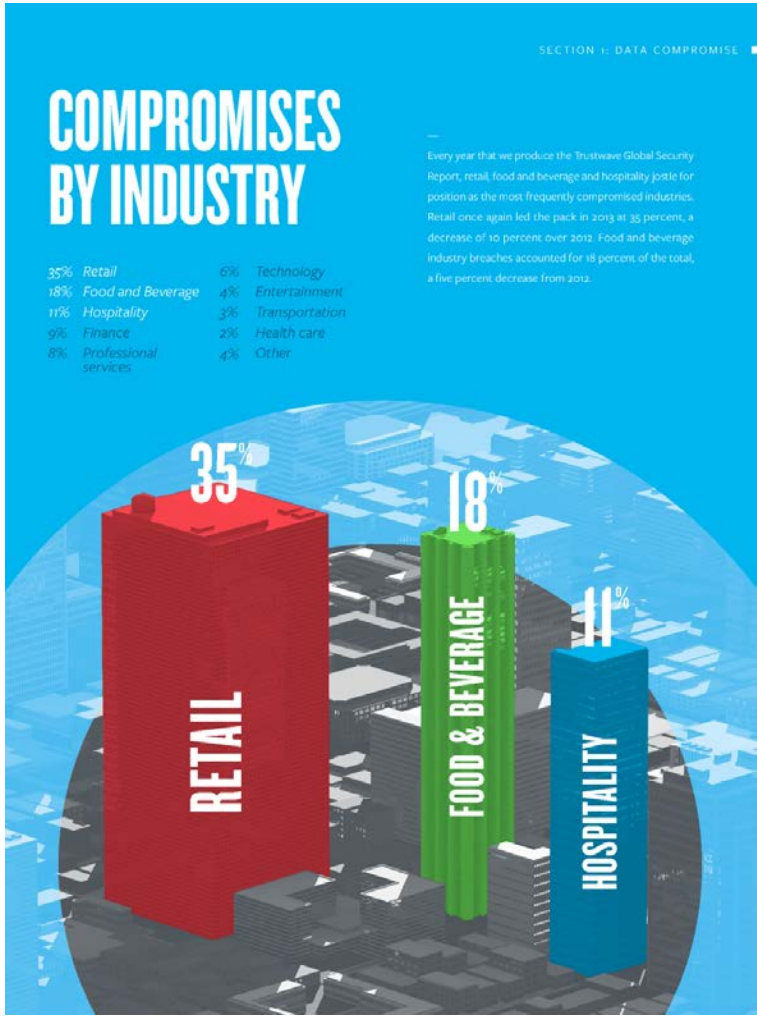


FMI

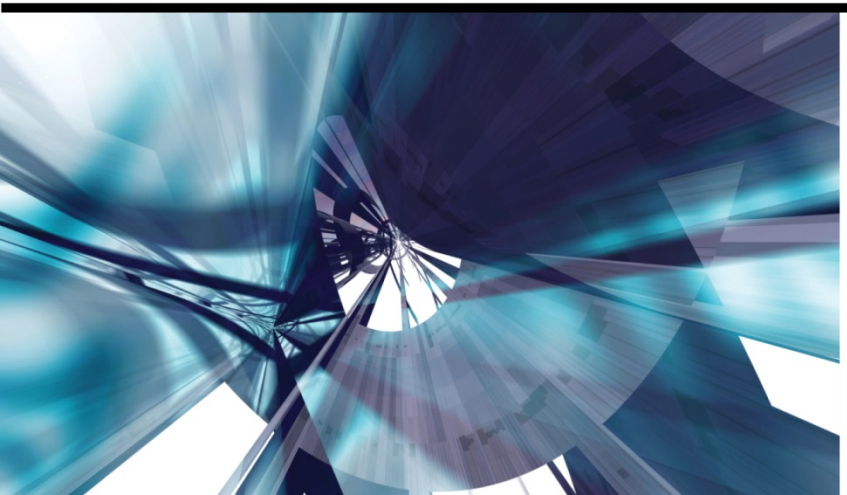
THE VOICE OF FOOD RETAIL

AVOIDING THE "NO PAY" POLICY

- Who is on your team?
- Lean on an experienced broker for exposure analysis, limit and structural advice
- Understand big picture (P&C market view, cyber insurance market), then your own insurance
- Be wary of sub-limits
- Understand the many nuances of PCI-related coverage
- Representation/warranty clauses and retro date
- Overly broad contractual liability exclusions
- Eliminate gaps in terrorism coverage
- Ask for enhancements generally found in D&O and other, more mature policies
- Look for and eliminate gaps for physical damage and/or bodily injury in other insurance; understand "other insurance"



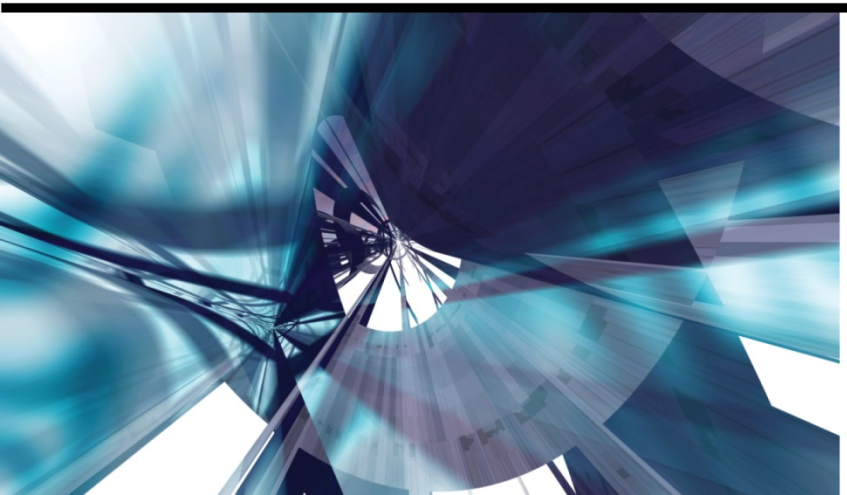
QUESTIONS?



FMI®

THE VOICE OF FOOD RETAIL

PEOPLE I PROPERTY I REPUTATION



FMI

THE VOICE OF FOOD RETAIL