AFP®
Annual Conference

Association for Financial Professionals®

OCTOBER 27–30, 2013 | LAS VEGAS

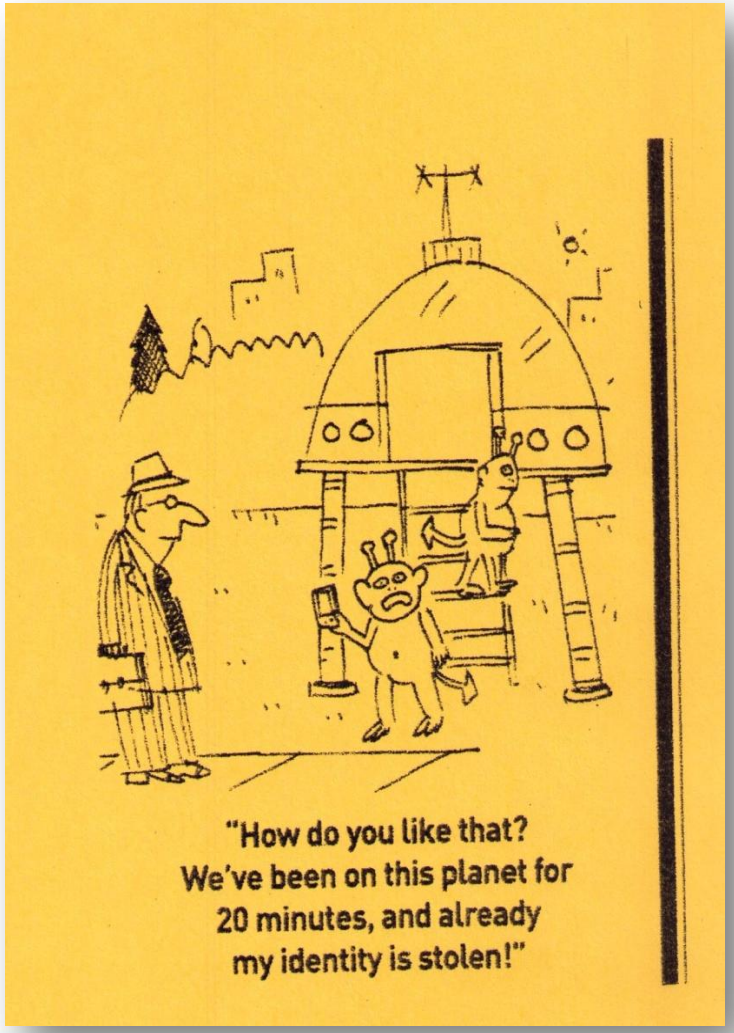
ORIGINAL→ESSENTIAL→UNBIASED→INFORMATION

Evolution of Cyber-liability: Mitigation

Kevin Kalinich, J.D.
Aon Risk Solutions
Global Leader-Cyber
Kevin.kalinich@aon.com

Cyber Exposures Mitigation Outline

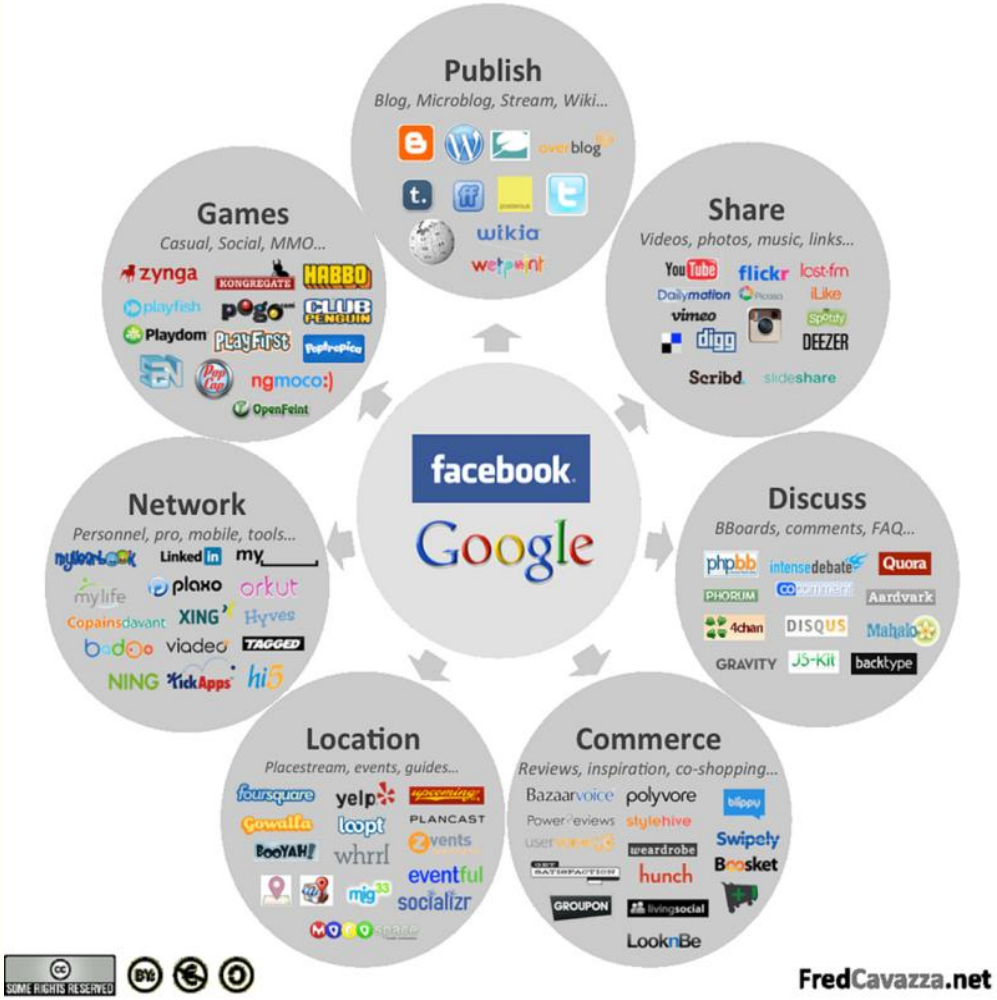
- **2013 Evolving Trends**
  - Financial Statement Impact
  - Board of Directors Issue
  - All Industries Impacted
- **Cyber Risk Identification**
  - Classify, Qualify & Quantify
- **Risk Mitigation**
- **Existing Insurance Policy Gap Analysis**

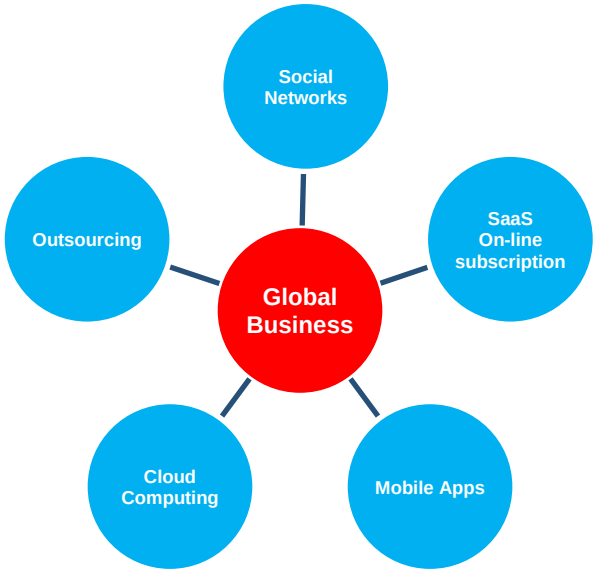


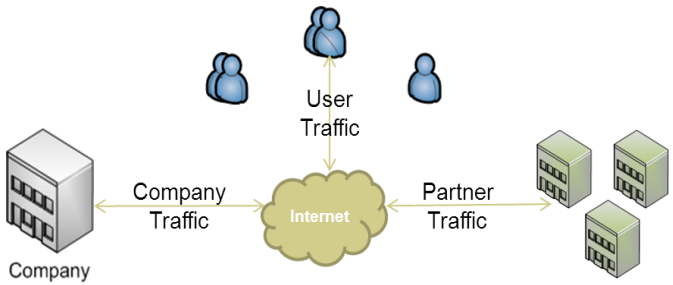
2013 Evolving Trends

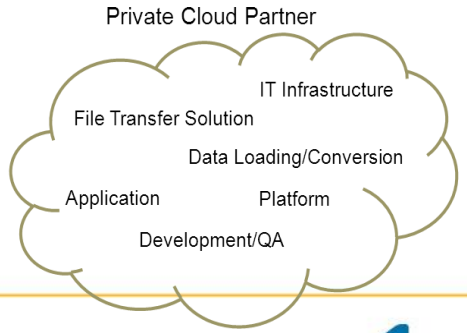
- **Increasing reliance on evolving technologies**
  - Mobile (including payments)
  - Cloud Computing
  - Social Media
  - Data Analytics (“Big Data”)
  - Third Party Vendor Issues
- **Payment Card Industry Data Security Standards: Fines & Penalties**
- **Data transfers in wake of NSA**
- **Cyber Risks Financial Statement Impact**
  - Actuarial Modeling
  - Board of Directors Liability?

E-Business Evolution





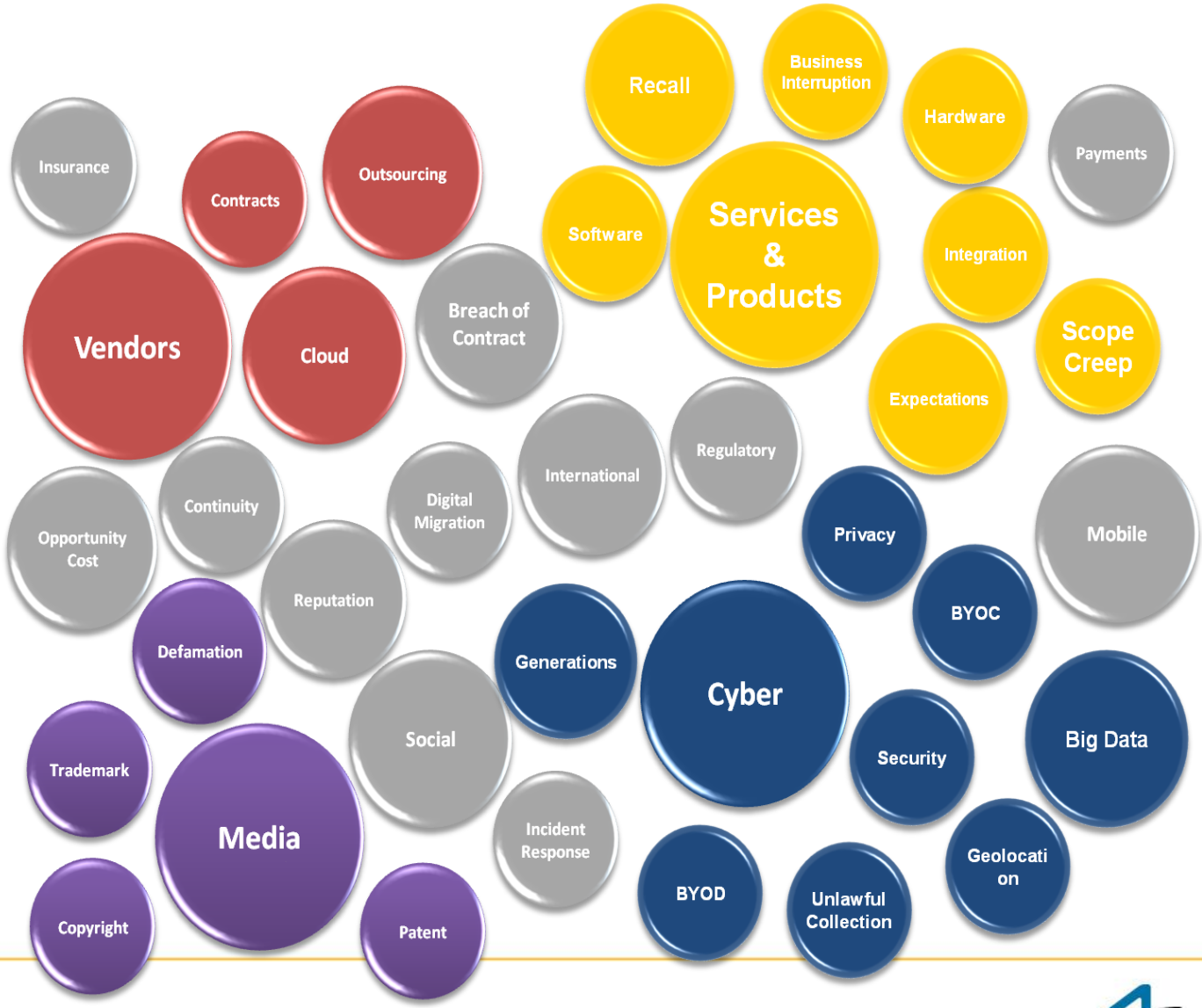




Cyber Risk Identification

- **Identify & Classify Cyber Exposures (online and offline – hard copy)**
- **Qualify**
- **Quantify**
- **Financial Statement Impact**
- **A Checklist for Corporate Directors and the C-Suite: Data privacy & Security Oversight (http://www.networkedlawyers.com/category/confidential-information-trade-secrets/)**

Exposure Analysis



Cyber Risk Discovery Process

Cyber Risk Actuarial Analysis growing

- **RISK vs. UNCERTAINTY**

- **RISK = Something you can put a price on**
- **(e.g. *exactly* 1 chance in 11 to hit an inside straight in Texas Hold'Em)**

- **UNCERTAINTY = risk that is hard to measure (e.g. Cyber exposure frequency & severity)**

- Review Comparable Cyber Losses
- Peer Benchmarking
- Monte Carlo Simulations
- Financial Impact Options
  - Risk Acceptance
  - Risk Avoidance
  - Risk Retention
  - Risk Transfer
    - Contractual Allocation
    - Cyber Insurance

- Risk mitigation is key in all cases
- Board of Directors Liability?????
- Integrate with Enterprise Risk Management

"We ignore the risks that are hardest to measure, even when they pose the greatest threats to our well-being"

-- Nate Silver, The Signal And The Noise: Why So Many Predictions Fail – But Some Don't

Risk Mitigation

- **Comprehensive Cyber Risk Mitigation Program: *Need Management Support***
- **Although IT Security & Use policies are important ----------it is MUCH MORE THAN AN IT SECURITY ISSUE**
- **Engage inter-departmental coordination and cooperation**
  - Risk Management
  - Finance/Treasury
  - Legal
  - Human Resources
  - CIO, CPO, CISO, IT Security
- **Education on Legal Exposures: train & monitor employees & all others**
- **Ensure Compliance with Organization's Privacy Policy regarding 3rd party Personally Identifiable Information**
- **Data Breach Management Policy – continuously update**
- **Third Party Exposures**
  - Vendor/Supplier Management
  - Contractual Considerations
  - Vendor/Supplier Audits

The Case for Risk Management

Ponemon 2012 Cost of a Data Breach Study

All of the below factors can either reduce or increase the cost of a data breach from its $188 per record average

Which ones hurt and which ones help?

What's the per record $$ impact of each factor?

- Notify customers ASAP
- Have a strong security posture
- Trust third party vendors with data, see it breached
- Have an incident response plan
- Hire an outside consultant to contain and resolve breach
- Appoint a Chief Information Security Officer
- Lose a laptop or other device (vs. other breach methods)

The Case for Risk Management

Ponemon 2012 Cost of a Data Breach Study

Factors that…

Decrease Breach Cost

Have an incident response plan - $42
Have a strong security posture - $34
Appoint a Chief Information Security Officer - $23
Outside consultant to contain/resolve breach - $13

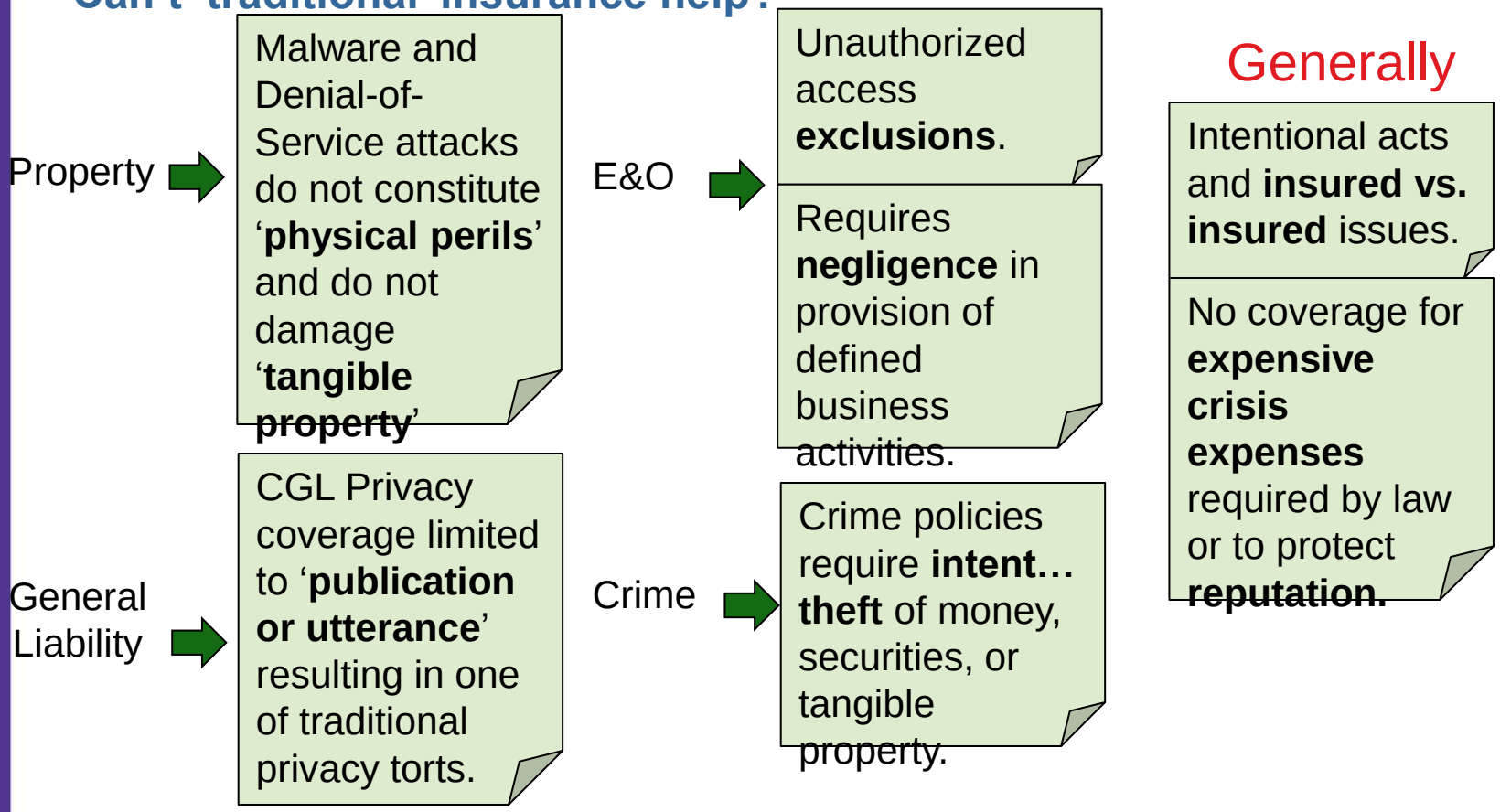
Increase Breach Cost

Trust third party vendors with data, see it breached + $43
Notify customers ASAP + $37
Lose a laptop (or other device) + $10

Sample 10 Questions To Ask

Question	Takeaways/Possible Conclusion
Do you have an Information Security Policy ?	Most will say yes. If no, it would suggest a lack of awareness of the issues and therefore would be unlikely to be ready for the product.
Is it based on any Information Security Standard?	Ideal answer would be ISO27002 as this is well understood and recognised by the market.
What is the Governance Structure for management IS Risk & Controls?	Presence of a structure is an indicator of a mature organisation who understands and is looking to manage the risks.
How do you maintain assurance of your internal IT controls ?	If there is an indication that a robust regime in place – a free scan should be positioned as additional assurance. No evidence is an opportunity for a free scan, but may also indicate a high risk.
Do you use third party suppliers?	Need for the product is increased if yes; need to find out the scope of services – if critical, need for cyber risk transfer is increased.
Do you obtain assurance of their Data/Security Controls?	Ideal answer is yes via a recognised method i.e. SSAE 16/SAS 70 or other auditing standard. These will be readily accepted as evidence.
What is your approach to the management of mobile devices?	Every client will have this issue; Laptop and device encryption are key controls. Lack of an informed response is not a good indicator.
What are your key controls to determine if are being subject to a cyber attack?	This provides an insight to the monitoring capability of the organisation. Most have poor levels of control unless they have outsourced a service.
Do you have a Cyber response team or plan?	Key area for extra service sales – most do not and failure to response quickly enough drives up and final incident cost.
Have you ever needed to complete a forensic examination of your IT equipment?	As above – often key evidence is destroyed through lack of awareness

Can't 'traditional' insurance help?



Potential Elements of Coverage in Commercial Property, General Liability, Crime, and Kidnap & Ransom Policies

Existing Coverage & Gaps

	Property	General Liability	Crime / Bond	K&R	E&O	Cyber
1st Party Privacy / Network Risks						
Physical damage to Data only						
Virus / Hacker damage to Data only						
Denial of service attack						
B.I. Loss from security event						
Extortion or threat						
Employee sabotage of Data only						
3rd Party Privacy / Network Risks						
Theft / Disclosure of private info.						
Confidential corporate info. breach						
Technology E&O						
Media Liability (electronic content)						
Privacy breach expense / notification						
Damage to 3rd party's Data only						
Regulatory privacy defense / fines						
Virus / Malicious code transmission						

Coverage Provided?	
Coverage Possible?	
No Coverage?	

** For reference and discussion only; policy language and facts of claim will require further analysis*

Existing Insurance Policy Claims Trends

- **Zurich v. Sony Declaratory Judgment Action: Over 55 class action lawsuits alleging billions of dollars in damages (Sept. 2011 new service agreement enforceable: mandatory arbitration and no class action?). Direct costs to companies impacted by cyber breaches, such as forensics, notification, credit monitoring and public relations costs, "are basic costs we would cover under our Zurich Security and Privacy Protection policy," says Zurich. Then if a claim is filed, "we have a liability coverage part that would cover the affected entity for defense costs and indemnity they have to pay out as a result."**

- **State National Insurance Co. v. Global Payments April 2013 $84 Million Declaratory Judgment Action regarding excess Professional Liability policy: Card association claims do not arise out of negligence from "professional services" or "technology-based services"**

- **Hartford v. Crate & Barrel and Children's retail Stores (Declaratory Judgment Action with respect to GL Policy):**
  - Over 125 Class Actions in California, lead by: ***Pineda v. Williams Sonoma***, 51, Cal.4th 524, 246 P.3rd 612 (Cal. 2011) (Zip codes are personal identification information protected by California's Song-Beverly Act)
  - Massachusetts Class Action: ***Tyler v. Michaels Stores, Inc.,*** No. 1:111-cv-10920-WGY (D. Mass. Filed May 23, 2011);.

- **Colorado Casualty Insurance Company vs. Perpetual Storage and the University of Utah (GL Policy) -- Negligence suit against insurance broker for not placing proper coverage**

- **Tornado Technologies Inc. v. Quality Control Inspection, Inc. (OhioCt. App. August 2, 2012) – no negligence of insurer for not warning insured to purchase special cyber policy**

- **Retail Ventures v. National Union Fire Ins. (August 23, 2012) Crime Policy Endorsement Applies**

- **Liberty v. Schnucks (August , 2013) Declaratory Judgment filed regarding General Liability policy**

Scope of Available Coverage

Mitigation

- Notification Costs
- IT Forensics
- PR + Advertising
- Credit Monitoring
- "Turnkey" breach response from carrier partners

Regulatory

- Regulatory Investigations
- Consumer Redress Funds
- Civil Penalties
- PCI – DSS Fines
- UK & EU country specific laws

Liability

- Individual Actions
- Consumer Class Actions
- Suits from business partners
- Suits from financial institutions

- Online and offline breaches
- Accidental or "rogue" employee actions
- Breaches caused by vendors or outsourcers

- **Coverage should be customized based on the nature of the business**
  - For example, FI consumer facing businesses can face a different liability chain (see recent ATM's)
- **Additional coverage available:**
  - 1st Party Business Interruption: Lost revenue due to failed network security
  - Information Asset: Loss or costs associated with restoring destroyed data
  - Cyber Extortion: Pays an extortion demand to a party that holds the Insured's system or data hostage
  - Media: Content based injuries (online and may include offline)

Insurance Underwriter Issues To Address

I. Contractual Allocation of liability and hold harmless and indemnity between Insured and each of each counterparties

II. Are all subsidiaries 100% wholly owned or are there joint ventures?

III. Does Insured comply with regulatory guidelines regarding disclosure of Cyber exposures, mitigation and risk transfer insurance (ADR's)?

IV. Review sample contracts from its suppliers as to allocation of liability, hold harmless and indemnity and insurance (name Insured as "Additional Insured?") We have set up "affinity" type programs for large players in the Financial Institutions space where a supplier of the FI can obtain a $1 MM E & O policy for the benefit of the Insured FI

V. Does Insured have any products or services that are protected from liability due to regulation? If so, what are the services and products and what are the revenues compared to total revenues?

V. Do we have a breakdown of revenue by each product/service as the exposures from each are different in both frequency and severity?

VII. What percentage of the products and services have been provided for over five years (at least 5 year's worth of Loss History)?

VIII. What percentage of products and services have been provided for less than one year?

IX. What type of internal or third party IT security assessments have been conducted? ISO 27001? SSAE 16?

X. What is the QA process for new products and services?

XI. What is the escalation process to approve contractual changes with customers?

XII. What is the escalation process to address and remedy complaints from customers?

XIII. What percentage of customers are business (B2B) vs. Individuals (B2C)?

Optimal Cyber Program