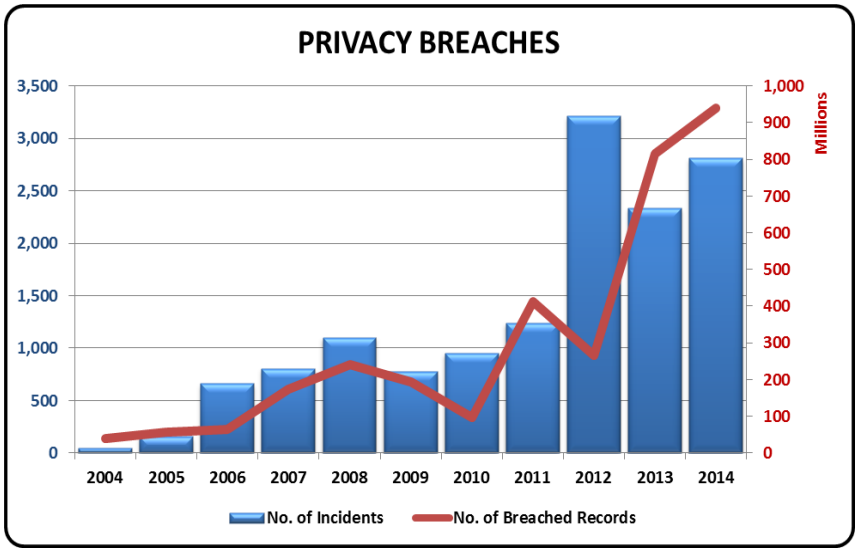
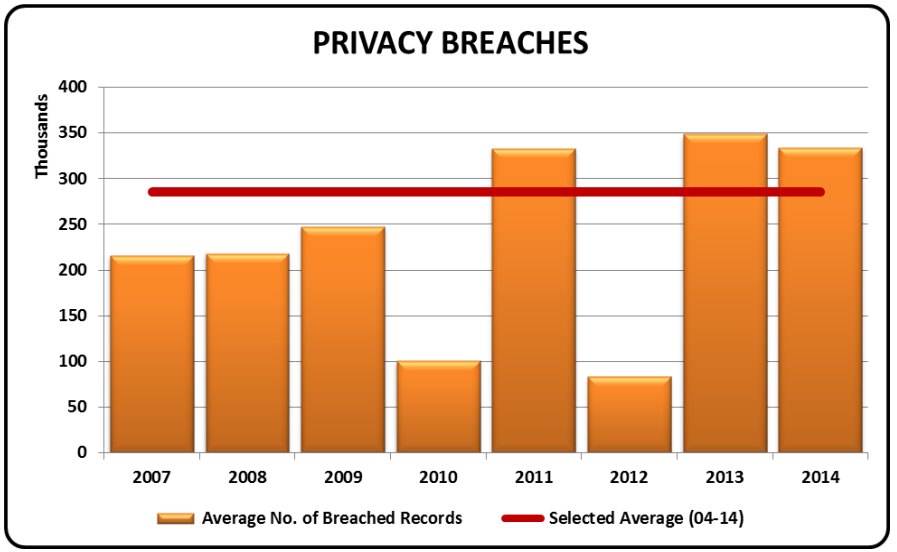
Network Security Privacy Liability and Insurance

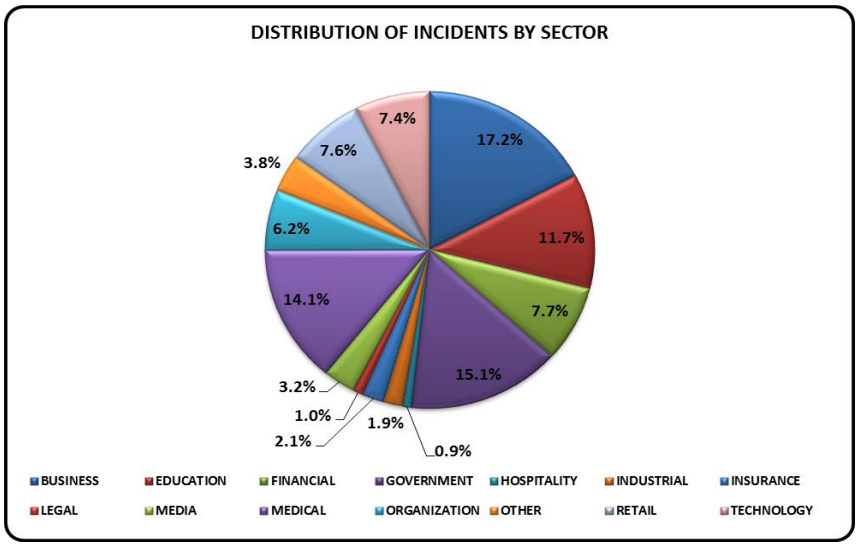
February 2015

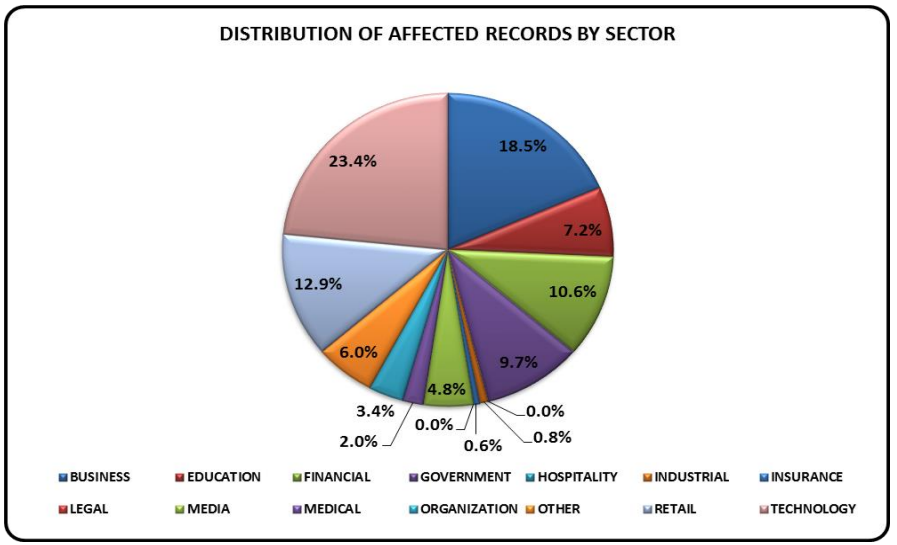
Willis

GLOBAL PRIVACY BREACHES*









*** Source: RiskBased Security -- Open Security Foundation – Data as of 12/31/2014.**

What is Different Today?

Familiar mediums

- SQL injections; spear phishing; malware, spyware & ransomware (“CryptoLocker”); denial of service attacks; web site defacing

New culprits

- Loosely formed groups of people who are very good at hacking and work together to do so (e.g., Anonymous, Lulzsec, Lizard Squad)
- State actors (China, Iran, US, Israel, Russia, North Korea, APT’s)

New information targeted

- Corporate data and trade secrets; inside information; embarrassing information; corporate weaknesses

New targets

- Automobile
- Internet of Everything
- Smartphones
- Medical Devices
- The Cloud

Network Security / Privacy Data Risk

What type of sensitive data do you collect?

- Personally Identifiable Information (PII)
  - Name, SS#, Address, Financial
- Protected Health Information (PHI)
  - Medical Information
- Employee data
- Corporate Confidential

Where is sensitive data stored?

How well is sensitive data protected?

How long do you store sensitive data?

What is a Data Breach Incident?

- Wrongful disclosure
- Unauthorized acquisition
- Security failure or Data compromised

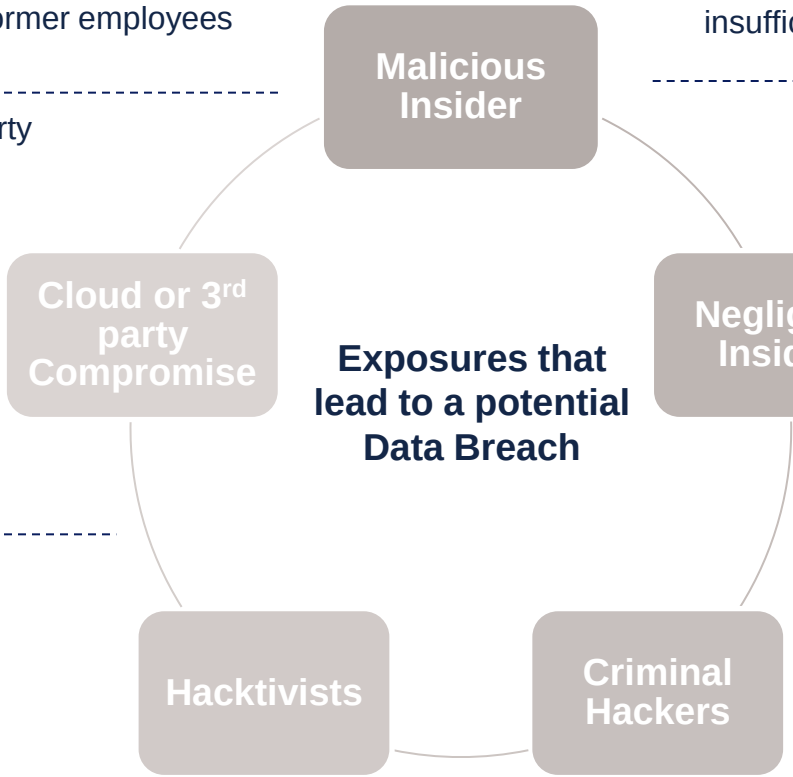
Can you survive a DDOS attack?
What about System Failure?

Sources of Potential Data Breaches

- Growing incentive for insiders to abuse access to sensitive data for financial gain
- Disgruntled current and former employees exploit back-doors

- Theft of Intellectual Property
- Security compromise – loss of sensitive client data
- Infrastructure downtime may lead to Dependent Business Interruption claim

- Intent is to disrupt and/or embarrass a target
- Motivations are fickle and unpredictable
- Massive DDoS attack



- Access controls and behavior monitoring insufficient to detect insider threats

- Unwary insiders susceptible to attacks that exploit traditional security controls (e.g. spear phishing)
- Users who fail to embrace "culture of security" will find ways to circumvent 'inconvenient' security controls

- Patience is a virtue. Tactics have evolved from "hit and run" to "infiltrate and stay."
- Industrialization - Black markets exist for all types of personal information
- Proliferation of mobile platforms and BYOD policies creates new vectors

Complex Regulatory Landscape

- State Laws/Regulation
  - Notification - 47 and counting
    - PII – Personally Identifiable Information – SS#, Account Numbers & PIN's, Name, Address, DL#'s, CC#'s
- Federal
  - HIPAA/HITECH
    - PHI – Protected Health Information – Insurance Claim Forms, Health Care Information, Explanation of Benefits, Notes, Conversations
  - FTC
  - SEC - OCIE/GLB/FINRA
  - EU Data Privacy Directive
  - Canada

- PCI-DSS compliance with Merchant agreement

Complex Regulatory Landscape - SEC

SEC/OCIE CYBERSECURITY INITIATIVE

The U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) previously announced that its 2014 Examination Priorities included a focus on technology, including cybersecurity preparedness.2 OCIE is issuing this Risk Alert to provide additional information concerning its initiative to assess cybersecurity preparedness in the securities industry.

OCIE's cybersecurity initiative is designed to assess cybersecurity preparedness in the securities industry and to obtain information about the industry's recent experiences with certain types of cyber threats. As part of this initiative, OCIE will conduct examinations of more than 50 registered broker-dealers and registered investment advisers focused on the following: the entity's cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats.

Complex Regulatory Landscape - FINRA

FINRA is conducting an assessment of firms' approaches to managing cyber-security threats. FINRA is conducting this assessment in light of the critical role information technology (IT) plays in the securities industry, the increasing threat to firms' IT systems from a variety of sources, and the potential harm to investors, firms, and the financial system as a whole that these threats pose.

FINRA has four broad goals in performing this assessment:

1.to understand better the types of threats that firms face;
2.to increase our understanding of firms' risk appetite, exposure and major areas of vulnerabilities in their IT systems;
3.to understand better firms' approaches to managing these threats, including through risk assessment processes, IT protocols, application management practices and supervision; and
4.as appropriate, to share observations and findings with firms.

Note: The assessment addresses a number of areas related to cybersecurity, including firms':

- approaches to information technology risk assessment;
- business continuity plans in case of a cyber-attack;
- organizational structures and reporting lines;
- processes for sharing and obtaining information about cybersecurity threats;
- understanding of concerns and threats faced by the industry;
- assessment of the impact of cyber-attacks on the firm over the past twelve months;
- approaches to handling distributed denial of service attacks;
- training programs;
- insurance coverage for cybersecurity-related events; and
- contractual arrangements with third-party service providers.

Complex Regulatory Landscape – DHS/NIST

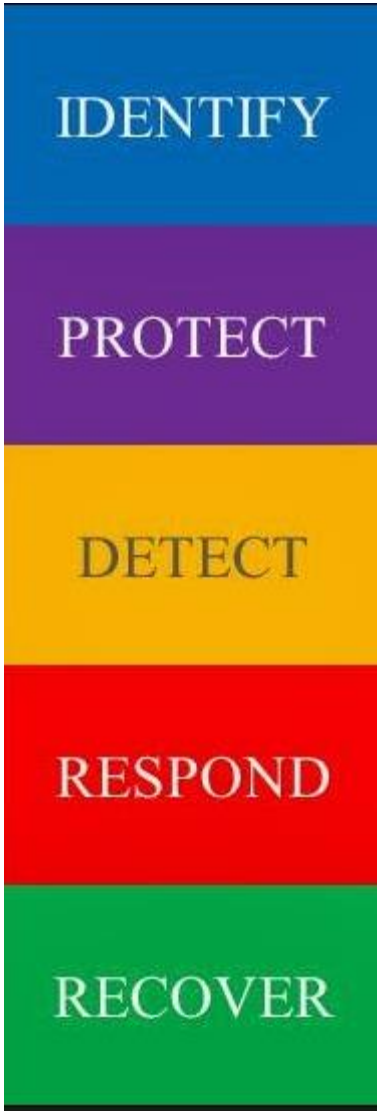
Cyber Security Voluntary Framework 2/2014

Originally designed for sectors that operate critical infrastructure, but increasingly used by others

Identifies five core functions of effective cybersecurity, which create a cycle of business processes towards cybersecurity: Identify, Protect, Detect, Respond, and Recover.

Advantages:

- Casts cybersecurity as part of enterprise risk, so that organizations can prioritize and invest in cybersecurity as part of their larger risk management strategy
- Creates a common vocabulary between business people (including directors) and technical personnel, and with third-party vendors
- Compliance with this national standard can help demonstrate due care by the board of directors or the company in subsequent litigation and to insurers
- The Framework may impact legal definitions of what actions are “reasonable” and enforcement guidelines for cybersecurity going forward



Stakeholders are Important – Why?

- Administration/Leadership Team

- Employees

- Residents/Customers/Clients

- CIO/IT/CISO

- Attorney General/General Counsel
- Chief Financial Officer

- Risk Management

What about the Board?

Five Principles that the Board should consider:

1. Cyber-risk is more than just an IT issue: it is a key component of enterprise risk management, requiring board-level oversight.

2. Cyber risks have important legal ramifications, which directors need to understand.

3. Cyber-risk should be a topic of regular board discussion, and boards need access to the expertise to engage with cyber-risk issues.

4. Directors should ensure management implements an effective cyber-risk framework for the company.

5. The board and management should assess cyber-risk just like other enterprise-level risks; ensuring a specific determination is made of which aspects of cyber-risk to accept, avoid, mitigate or insure against.

NACD Report 2014

Data Breach Consequences

Third and First Party Claims

- Notification and Call Center costs
- Legal – “Breach Coach”
- Computer Forensic Investigation
- Credit Monitoring & ID Theft costs
- Public Relations/Crisis Management
- Regulatory penalties and fines
- Class Action suits
- Legal Defence costs:
  - Civil, regulatory and possibly criminal defense
  - Data Privacy counsel can cost $500 per hour. A major data breach will cost millions in legal costs
- Business Interruption Costs/Data Damage

Privacy/Network Liability Coverage

Liability Coverage

- Privacy Liability
- Network Security Liability
- Media and Content Liability
- Regulatory Liability
- Technology E&O

Direct (Loss Mitigation – First Party) Coverage

- **Data Breach Expenses:**
  - ✓ Notification, Forensic, Credit Monitoring/ID Theft Monitoring, Public Relations expenses, Legal “Breach Coach”

Direct (First Party) Coverage

- Business Income Loss (Network Security)
- System Failure
- Data Reconstruction
- Extortion Costs

Type of Coverage

3rd Party Coverage

Network and Privacy Liability

- *Coverage for:*
  - Claims arising from the unauthorized access to data containing identity information,
  - Failure to protect non-public information (PII/PHI/Corporate Confidential Information in your care, custody and control,
  - Transmission of a computer virus, and Liability associated with the failure to provide authorized users with access to the company's website

Media Liability – Including online and offline Media

- *Coverage for: Claims arising online/offline content*
  - Libel
  - Slander
  - Defamation
  - Emotional Distress
  - Infringement of copyright/trademark/etc.
  - Invasion of Privacy

Type of Coverage

3rd Party Coverage

- Regulatory Liability
  - *Coverage for:*
    - State/Federal/International fines & penalties

- Technology Products/Services Errors & Omissions
  - *Coverage for:*
    - Claims arising from the failure of a technology product or service to perform as indicated.

Type of Coverage

1st Party Coverage

- Crisis Management/Security Breach Remediation and Notification Expenses
  - *Coverage for:*
    - *Crisis Management Expenses* Covers expenses to obtain legal assistance to navigate the event, determine which regulatory bodies need to be notified and which laws would apply
    - Public relations services to mitigate negative publicity as a result of cyber liability
    - Forensic costs incurred to determine the scope of a failure of Network Security and determine whose information was accessed
    - Notification to those individuals of the security breach
    - Credit monitoring
    - Call center to handle inquiries
    - Identity fraud expense reimbursement for those individuals affected by the breach

Type of Coverage

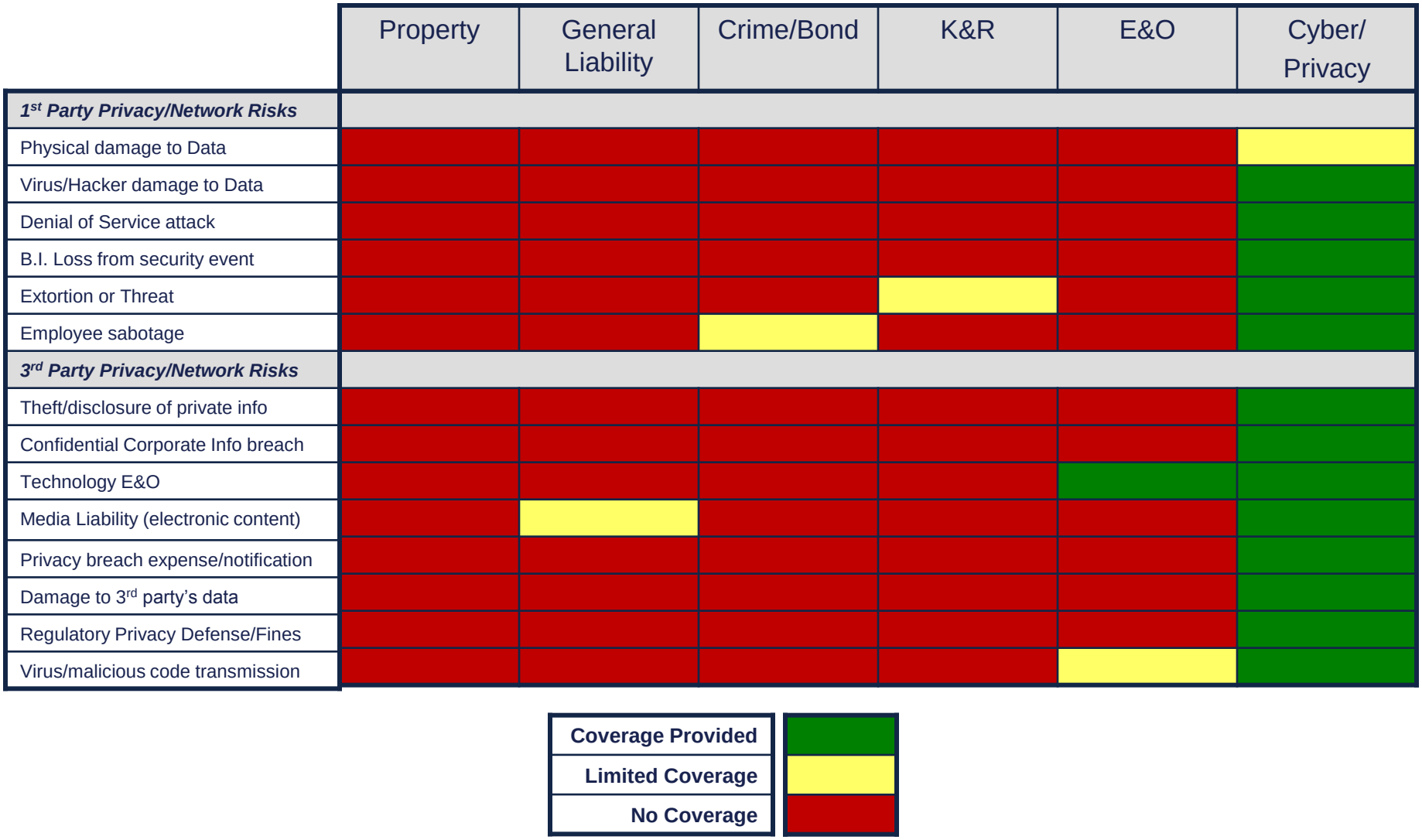
1st Party Coverage

- Computer Program and Electronic Data Restoration Expenses
  - *Coverage for:*
    - Expenses incurred to restore data lost from damage to computer systems due to computer virus or unauthorized access

- Cyber Extortion
  - *Coverage for:*
    - Money paid due to threats made regarding an intent to fraudulently transfer funds, destroy data, introduce a virus or attack on computer system, or disclose electronic data/information

- Business Interruption and Additional Expense
  - *Coverage for:*
    - Loss of income, and the extra expense incurred to restore operations, as result of a computer system disruption caused by a virus or other unauthorized computer attack

Cyber Risk Gaps in Traditional Insurance



Coverage Provided
Limited Coverage
No Coverage

Cyber Insurance Markets

A Maturing Market:

- Over 60 insurers writing coverage – a very robust market
- Substantial claims paid without insurers withdrawing from market
- Recognized underwriting standards
- Estimated $1B premium volume moving to $5B

- **VALUE – EXPERTS, PROFESSIONALS, RE-ACTIVE & PRO-ACTIVE**

Sample Markets:

- ACE
- AXIS
- Beazley
- AIG
- Zurich
- C.N.A.
- AWAC
- Travelers
- Chubb
- AEGIS
- HCC
- Torus
- Ironshore
- Liberty
- Navigators
- One Beacon
- RLI
- Swiss Re
- Hiscox
- XL
- London Markets

Our Differentiators

- **Insurance Program Gap Analysis**
  - Assess and outline the gaps or deficiencies in your traditional insurance policy, highlighting those areas potentially addressed in a cyber policy

- **Analytics Trifecta**
  - Data Breach Calculation
    - Using Willis Data Breach calculator, we assess your potential breach costs
  - Peer Group Benchmark
    - Utilizing basic placement details we are able to provide you with a comparison of basic program features against relative peer companies
  - PRISM Analysis – Privacy Risk Insurance Strategy Model using CCoR
    - Conduct analytics based on Monte Carlo Simulation to model loss probability and program comparisons. This help clients decide how much cyber insurance would provide value for the premium spent

Our Differentiators

- Willis is focused on being the broker authority in the Cyber space
- Team of 20 professionals within the U.S. focused on cyber
- Developed proprietary models to assess privacy risk & limit adequacy
- Dedicated cyber claim professionals that work with you to ensure your event is being handled properly
- Proactive assistance in evaluating your individual needs, risks and exposures
- Collaborate with your team on manuscript language to ensure your specific operations, risks and exposures are covered properly
- Provide contractual advise and guidance related to cyber issues with customers, partners and vendors
- Assist with Executive and Board presentations

For More Information

Contact:

Joe DePaul

Willis FINEX Cyber & E&O National Team

(212) 915 7945

joe.depaul@willis.com