Cyber Insurance

Presented by Ronald Tafoya, RESPEC and Becky Tafoya, PNMR

Public Meeting

April 2018

Presenters

- Rebecca Tafoya

- Rebecca Tafoya has 25+ years of experience in the insurance industry. She joined PNM Resources, Inc. in 2015 to manage the corporate insurance functions including the insurance structure, enterprise risk management and implementation of risk transfer mechanisms for Public Services Company of New Mexico and Texas New Mexico Power.
- Prior to joining PNM Resources, Inc. Rebecca was the Executive Director for Integrion Group, Inc. the largest Third Party Claims Administration and Independent Claims Adjusting Company in New Mexico and now a regional company doing business in Arizona. Integrion Group is a wholly owned subsidiary of New Mexico Mutual which is the largest Workers' Compensation carrier in New Mexico. From 2004 through 2013, Rebecca was the Deputy Risk Management Director for New Mexico Association of Counties where she managed three self-insured Pools for Workers' Compensation, Multiline and Law Enforcement.
- Rebecca graduated from New Mexico State University in 1981 with a B.S. degree in Business Administration and earned her Associates in Risk Management (ARM) with an emphasis in Public Entities from the American Insurance Institute in 2008.

Presenters

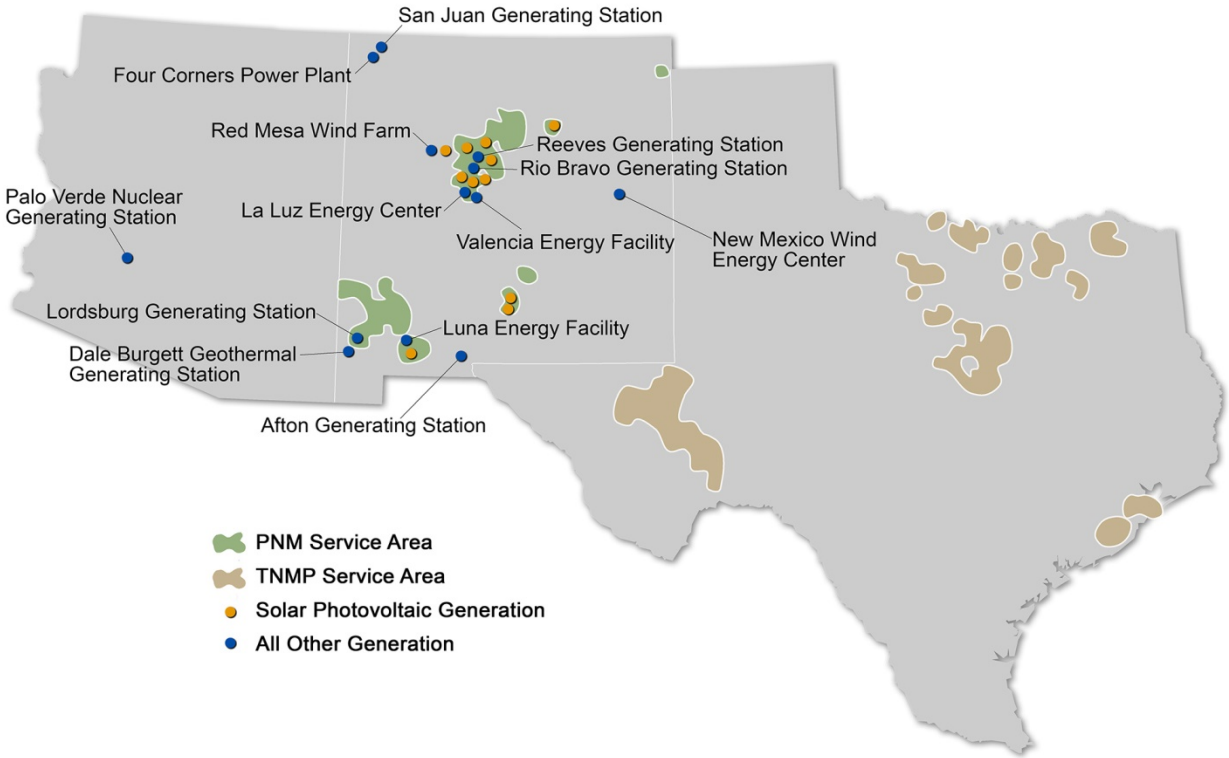
- Ronald Tafoya

- Ron Tafoya is a Principal Consultant at RESPEC working in the Data and Information service area of the company and focused on Cyber Security. He is also the Technologist in Residence for a high technology business accelerator located in New Mexico called the High Desert Discovery District (HD3).
- Previously he was the Security Champion for the Intel Non-Volatile Memory Solutions Group (NSG). He was with Intel for 16 years. As the Security Champion for NSG, he was responsible for the security all NSG products, which included all Intel Solid State Drives. He has more than 25 years of professional experience in all aspects of computer software application development and deployment and has focused on cyber security for over 20 years.
- He is a certified Project Management Professional (PMP), he is a Certified Ethical Hacker (C|EH), and is a Certified Information System Security Professional (CISSP). In addition to his security experience, he also has broad experience in small business development and technology and has held various other positions such as the Senior Project Manager for the National Center for Gnome Research and the Technology Enterprise Division Director in the New Mexico Economic Development Department. He is active in Infragard, and several other local and national security organizations and also sits on various boards for public and private sector organizations. Follow him on Twitter @rtafoya, on LinkedIn at https://www.linkedin.com/in/rontafoya, or on his blog at http://goo.gl/gsLZmE.

PNM Resources Overview

PNM Resources is a regulated electric utility holding company focused on providing environmentally responsible, affordable and reliable electricity to customers and above industry average earnings and dividend growth to shareholders

Generation Resources and Service Territories



PNM Resources

- Energy holding company
- Based in Albuquerque, New Mexico

PNM

- Located in New Mexico
- 520,449 customers
- 15,049 miles transmission and distribution lines
- 2,791 MW generation capacity
- Top quartile reliability
- Affordable rates

TNMP

- Located in Texas
- 246,620 end-users
- 9,298 miles transmission and distribution lines
- Top quartile reliability
- Affordable rates

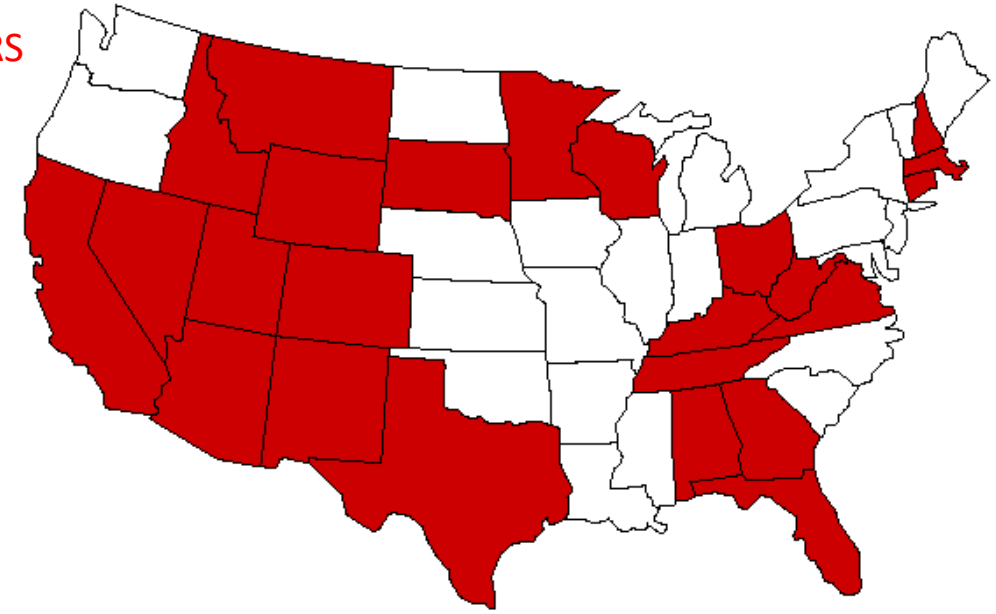
RESPEC Overview

RESPEC is a 100% ESOP - Our Employees own the company. We all have a vested interest in our future.

RESPEC DTS Overview

BY THE NUMBERS

- Over 280 Employees
- Over 20 Office Locations
- $40M in annual revenue
- RESPEC was incorporated in 1969 in South Dakota



RESPEC has provided client-directed IT staff and project based services in 24 states.

RESPEC

- RESPEC's Data and Technology Solutions (DTS) division provides technology solutions, products, and staffing services for public and private clients across various industries.
- Our goal is to ensure that the technology our clients use is aligned with their business objectives.
- We have 120+ IT Professionals that bring a 360-degree approach to providing business and IT solutions

Expertise in 9 major areas of IT solutions:

- Business Process Reengineering
- Independent Verification & Validation (IV&V)
- Systems Integration
- Data Management
- Application Development
- Geospatial Information Systems (GIS)
- Billing & Revenue Management (BRM)
- Cybersecurity & Accessibility
- Staff Augmentation

Cybersecurity Insurance - Agenda

- Cyber Insurance Predictions, Cyber threat landscape and risk challenges.
- What Role Should Cyber Insurance Play in Your Risk Management Strategy?
- Collaboration between Risk, IT And Everyone Else: How Do I Understand My Risk Profile?
- Getting Board Buy-In: How Do You Sell Cyber Insurance Internally?
- Making Cyber Insurance A Reality: Where Cyber Insurance Does And Doesn't Help.
- Cybersecurity Insurance Market Trends

Cyber Risk Predictions

The cyber threat landscape continues to intensify and the impact of **cyber attacks expected to continue to increase**

Cyber risk can **no longer** be effectively managed solely as **an IT issue**

A shift to Manage Cyber as an Enterprise Risk

- Companies increased reliance on IT
- Regulator's focus on protecting consumer data
- The value of non-physical assets

Cyber exposures will require **security** to be **integrated** into both **business culture and risk management framework**

Cyber Threat Landscape

Average cost of a data breach

increased from

$3.9 to $4M

2016 Ponemon Cost of Data Breach Study: Global analysis

Global Loss

$445B

CSIS Center for Strategic and International Studies

Cost

$2.5B

In insurance **premiums**

Threats

430M Pieces of unique malware increased **36%**

35% increased in ransomware

554M records compromised

Systemic Internet Security Threat Report (April 2016)

Connectivity

20.8B connected devices

1,555 individual partners

$86.4B spent on security in 2017, **up 7%** from the previous year

Cyber Risk Exposures – Challenges

Cyber threats are predicted to continue to **evolve and increase** endangering a company that can't keep pace.

Organizations are under pressure to **refine** their **defenses** against **attackers** who are **constantly advancing** their techniques.

Regulators are trying to **keep pace** further complicating an organization's risk management approach.

Organizations should commit to a **continuous process** of **evaluation** and **improvement.**

Regular assessments, testing, refinement, and responsiveness are essential to **keeping critical assets protected** and **ensuring strong governance** and compliance.

Organizations need to be constantly focused on **limiting** the **economic** and **reputational damage** from cyber incidents.

What Role Should Cyber insurance Play in Your Risk Management Strategy?

- Today's Silo driven approach to cyber risk management is changing to a coordinated C-suite driven approach to **address cyber risks holistically across all functions of the enterprise.**
- Cybersecurity needs to become **operational.**
- **Protecting the crown jewels:** Do you know your most valuable assets?
- A strong cyber-risk management strategy should take account of the **wider cyber landscape.**
- Collaboration between In-house cybersecurity function and Managed Security Operations Center (MSOC) is key.
- Understanding of what attackers want, what most needs protection, your **tolerance to incidents** and clear roles and responsibilities of each person in your organization.

Cybersecurity Risk Management, Cont.

- Align your cyber enterprise risk management strategy with your corporate culture and **risk tolerance.**
- If I transfer, how much coverage do I need and how much cyber **insurance limits** are available?
- Examine **existing insurance policies** and consider changes that **expand or clarify coverage** for possible cyber claims (General Liability, Crime, Property, D&O, Technology E&O).
- As companies turn to **tailored enterprise cyber insurance policies**, insurers will likely limit coverage of cyber-related losses in traditional property, casualty, and other business policies.
- Define all the above in your **cybersecurity policy.**

Cyber Insurance - How Do I Understanding My Risk Profile?

Collaboration Between Risk, IT and Everyone Else

- Requires companies to **shift managing cyber risk** from a silo-driven approach to an **enterprise risk**.
- Coordinated C-suite driven approach to the impact of cyber risk **holistically across all function of the enterprise**.
- **Cyber Governance**: Directors and Officers can be held personally responsible for the handling of cyber attacks.
- **Regulatory pressures** will continue to intensify with renewed enforcement on compliance and audit against the impact of cyber attacks.
- **Chief Risk Officers** working with **information security teams**, **treasurers, chief financial officers** (CFOs) and **legal** to improve risk modeling and understand the **holistic business exposures**.

Cybersecurity Insurance – How Do I Understand My Risk Profile

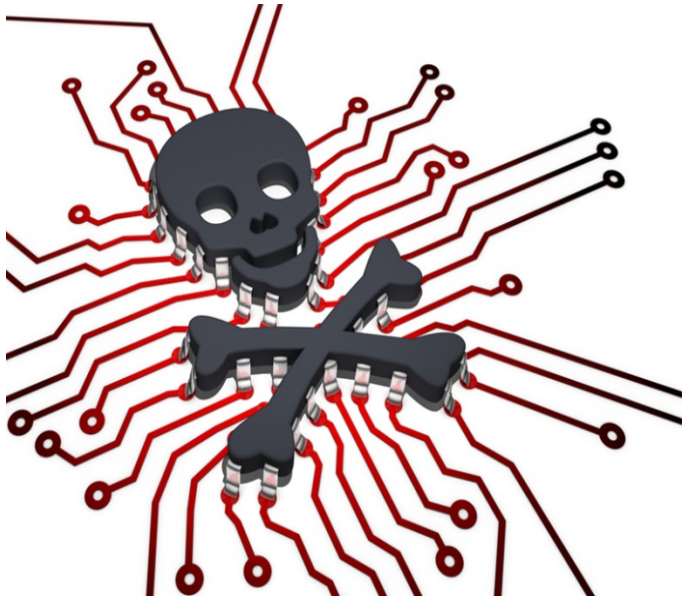
Questions Board of Directors Should Consider:

- ✓ What are the companies **highest valued data assets?**
- ✓ Where are the data assets located?
- ✓ How are those assets protected?
- ✓ What are the greatest threats to data assets?
- ✓ Who are the potential threat actors?
- ✓ What is the worst case scenario?
- ✓ Have we performed appropriate Risk Assessments and Penetration Testing?
- ✓ Do we have the appropriate and most updated **Data Privacy /Security Policies** in place?
- ✓ Do we have an **Incident Response Plan** (IRP)?
- ✓ How will the IRP respond to a major attack?
- ✓ Who are the **members of the Incident Response Team** (IRT)?
- ✓ Has the IRT **performed Table Top exercises** to test the IRP?
- ✓ What due diligence is performed with regard to **third party service providers/ vendors?**
- ✓ **What training is in place for employees?**
- ✓ Does employee training protocols cover mock spear-phishing attempts?
- ✓ Are the appropriate Access Controls in place?
- ✓ What type of Anti-Virus, Intrusion Prevention/Detection Systems are in place?
- ✓ Do we have an effective process for patching and scanning for vulnerabilities?
- ✓ What Cyber Security Frameworks are in place?
- ✓ Have we engaged outside **data privacy counsel**?

How likely is a Cyber Attack on your Company, and is your company prepared?

2017 Score Card: Are you protected?

- Criminals harness IoT devices as botnets to attack infrastructure.
- Nation state cyber espionage and information war influences global politics and policy.
- Data integrity attacks increased.
- Spear-phishing and social engineering tactics become more crafty, more targeted and more advanced.
- Regulatory pressures make red teaming the global standard with cybersecurity talent development recognized as a key challenge.
- Industry first-movers embrace pre-M&A cybersecurity due diligence.
- **You can't stop all cyber attacks. It's not a question if, it's a question of when.**



Risk Assessment Process

Cybersecurity Insurance – Risk Assessment

Threats

- Bot-Network Operations
- Criminal Groups
- Foreign Intelligence Services
- Hackers and Hacktivists
- Insiders
- Spear-phishing and social engineering
- Spammers
- Spyware/Malware
- Terrorists

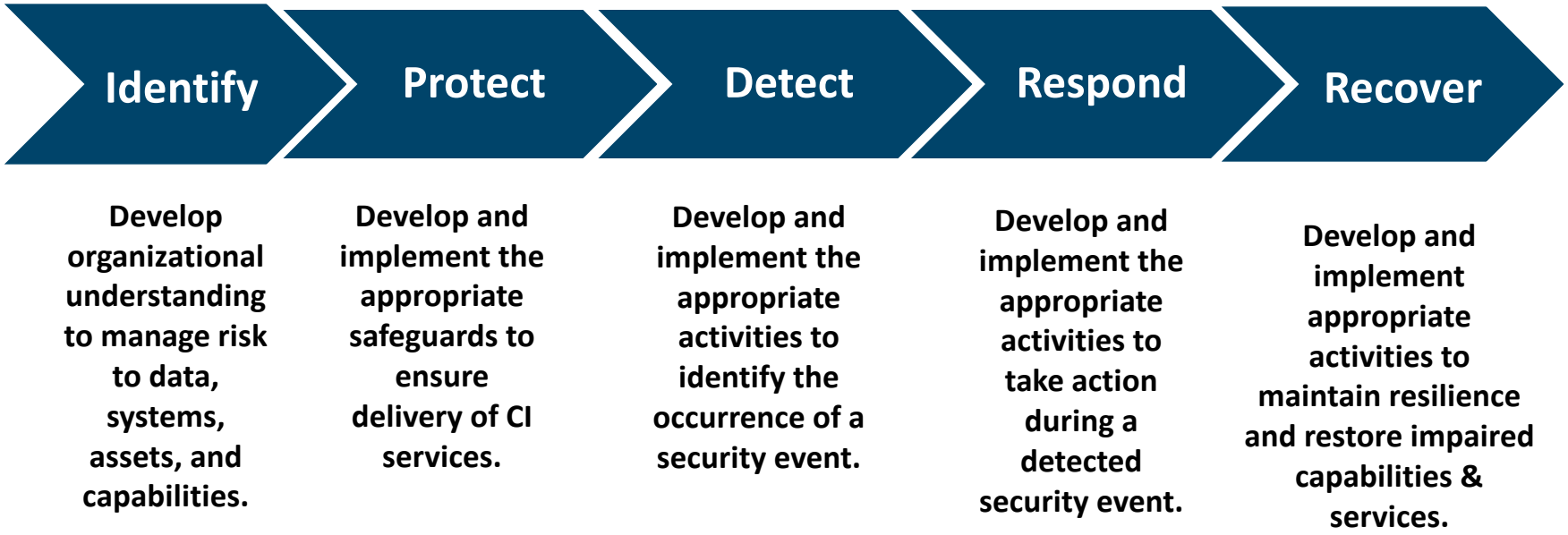
Challenges

- You don't known you have been compromised
- Unaware employees
- Cybersecurity talent development
- Antiquated Infrastructure
- Evolving Technologies
- Regulatory pressures
- Cybersecurity due diligence
- Cyber Governance

Cybersecurity - Risk Prevention

NIST Cyber Security Framework

The National Institute of Standards and Technology (NIST) Cyber Security Framework was created in response to President Obama's Executive Order 13636, "Improving Critical Infrastructure Cyber Security", for companies involved in the delivery of CI services.
https://ics-cert.us-cert.gov/Introduction-Recommended-Practices



Cybersecurity - Risk Prevention

- The CRO should work closely with CISOs to help company leadership **understand the holistic impact of cyber risk across the enterprise.**
- Proper treatment of these risks requires a layered approach and a combination of risk management techniques including **risk avoidance, contractual transfer, risk retention, risk control and risk transfer.**
- Risk control techniques must not only include **Technology Controls but People and Process Controls**.
- Employee cyber security awareness training and **adopting an actionable framework**, such as NIST can significantly mitigate risks.

Cybersecurity – Where Cyber Insurance Does Help

Cyber insurance is currently a stand-alone product but moving to a future **where all classes of risk and insurance will be touched by a cyber event.**

Cyber-insurance cannot protect your company from a cyber-incident. However, cyber insurance can provide some measure of **financial support** in case of a data breach or cyber-incident.

Cyber insurance underwriting process will identify and **protect your critical assets and balance sheet** by aligning your cyber enterprise risk management strategy with your **corporate culture and risk tolerance.**

Cybersecurity – Where Cyber Insurance Does Help

Cyber insurance assist in funding potential breach response expenses: **Business interruption losses, extortion expenses, defense costs for third-party lawsuits and regulatory actions, state and federal fines/or penalties and other costs and liabilities.**

Cyber insurance can provide useful information for **assessing your risk level and identifying cybersecurity tools and best practices** that you may be lacking.

Cyber insurance and the associated **underwriting processes can strengthen your cybersecurity controls.**

Where Cyber Insurance Does Help

Cyber Insurance - Covered Events

- Computer Crime and Computer Attacks
- Administrative or Operational Mistakes
- Accidental Damage or Destruction
- Security, Privacy & Multimedia Liability
- Network Asset Protection
- Cyber Extortion and Terrorism

Cyber Insurance - Coverages

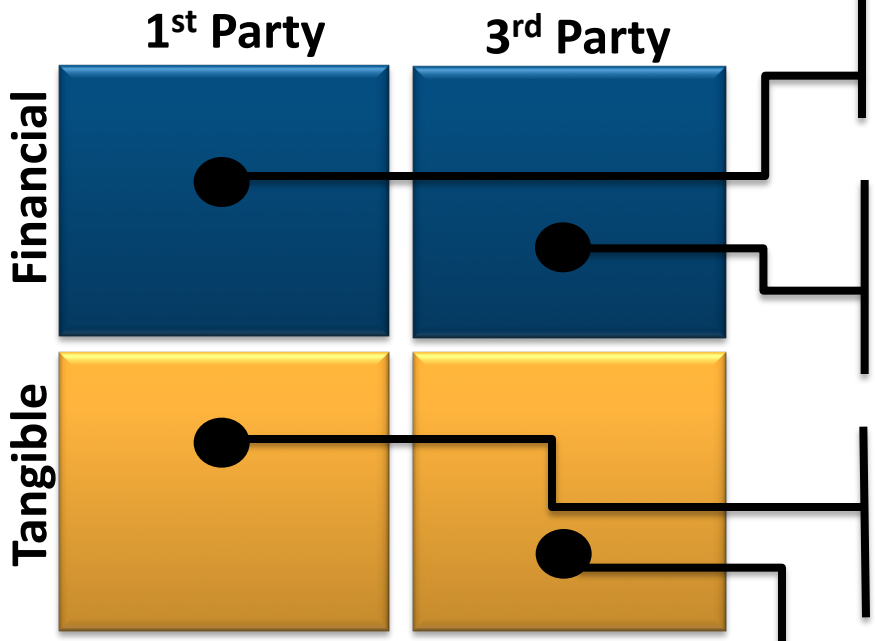
- Extortion monies
- Crisis Management
- Forensic Research & Repair
- Defense Counsel experts in cyber attacks
- Fines and penalties
- Expenses: Notifications, credit monitoring, call center monitoring, ID theft restoration & repair, data breach coach, legal counsel and remediation expert
- Extra Expenses: business interruption, liquidated damages, rental of office space or equipment, etc.

Where Cyber Insurance Doesn't Help

- **Reputational harm and loss of trust** by shareholders, customers and regulators.
- **Class action lawsuits** impact to Liability, D&O, Crime or Property insurance policies.
- **Inability to collect receivables** due to compromised financial systems.
- **Wrongful Acts by employees**.
- **Executives/Board of Directors** forced to resign as a result of a cyber attack.
- Interruptions and financial impact to t**hird-party vendors and suppliers**
- Cost of response on a **Threat that never materializes**

Cybersecurity Insurance –Risk Assessment

Cybersecurity Insurance - Risk Impacts All Loss Quadrants



Any major cyber event will result in

- Public relations, response, and continuity costs
- Immediate and extended revenue loss
- Restoration expenses
- Defense Costs

Third parties will seek to recover

- Civil penalties and awards
- Consequential revenue loss
- Restoration expenses

Physical damage is now possible

- 1st party property damage
- 1st party bodily injury

Physical damage may cascade to others

- 3rd party property damage
- 3rd party bodily injury

Cyber Insurance Coverage Available in the Marketplace

Defense Costs + Damages + Regulator Fines

Liability Sections

- Failure of Network Security
- Failure of Protect/ wrongful Disclosure of Information, including employee information
- Privacy or Security related regulator investigation
- All of the above when committed by an outsourcer
- Wrongful Collection of Information
- Media content infringement/ defamatory content

Insured's Loss

First Party Sections

- Network-related Business Interruption
- Extra Expense
- Dependent Business Interruption
- Data recovery
- System Failure Business Interruption

Expenses Paid to Vendors

Expense/Service Sections

- Crisis Management
- Breach-related Legal Advice
- Call Center
- Credit Monitoring, Identity Monitoring, ID Theft Insurance
- Cyber Extortion Payments

Getting Board Buy-In: How Do You Sell Cyber Insurance Internally?

- Present your **risk profile**, identify cyber **risk exposures** and **potential impact** (liability, financial and operational).
- **Cyber risk trends** and benchmarks specific to your industry.
- **D&O liability** claims over cyber incidents hold board members personally responsible.
- Cyber events rank among the top 3 triggers for **D&O derivative actions** and expected to intensify in 2018.
- Understand the impact of a cyber attack that can result in **added expenses, reduced earnings, class action lawsuits, regulatory investigations, regulatory penalties and fines and reputational risk.**
- Determine your Boards of Directors **cyber risk appetite**.

Cybersecurity - Insurance Market

According to 62% of brokers, Cyber coverage is becoming more consistent, but it is still difficult to compare policies

Pricing is seen as **less consistent** than last year, many brokers noting soft market conditions and broadening coverage without adequate rate consideration

Market expands as existing insureds continue to buy more coverages and higher limits at renewal

The Dyn DDoS attack and WannaCry ransomware attack had slight to no impact on underwriting and/or pricing for **71%** of respondents

News of a loss continues to be the main driver for cyber insurance purchase

Healthcare still leads the new buyers list, but other industries are catching up

Over **80%** noted buyers switching from Cyber endorsements to stand-alone policies – **43%** noted that this occurred frequently

Cybersecurity – Insurance Market

Market is split on whether cyber-related property damage should be covered by a Property policy **(44%)** or Cyber policy **(40%)**

More than half of the respondents felt that Social Engineering losses (funds transfer fraud) should be covered under a Crime policy

24% of respondents felt that the GDPR would have a significant impact on the take up rate of Cyber insurance in Europe

Not understanding the exposures and coverage remain as the main obstacle to purchasing Cyber insurance

Cybersecurity – Insurance Market

The Changing Cyber Insurance Market

- Cyber insurance markets continue to mature and become **specialized and innovative**
- New Cyber trends continue to emerge and represent **new challenges and developments in cyber risks** and security landscape.
- Cyber risks have become more **systemic as connectivity continues to grow**.
- The **impact of worst-case scenario's** as a result of a cyber event continues to rise.
- The next wave of cyber insurance growth is the result of new **privacy and regulation** in the U.S.
- Insurance markets underwriting process will require companies demonstrate they have addressed cyber risks and have **best practices** in place to protect assets, consumers and employees.

Cyber Insurance Purchase Considerations:

- Many companies still lag on fundamental **risk assessment and mitigation measures**, and hackers are perpetually refining the tools in their cybercrime arsenal to stay several steps ahead.
- Insurance markets are starting to be more consistent in coverages offered as they pertain to cyber, however there is still a very wide variety.
- Market capacity is still limited. Seek a mature carrier.
- Competition is driving down pricing. Competition between carriers was seen to prevail over actuarial assessment of the cost of risk. **It's "becoming a sales game, rather than the pricing of risk.**
- **Insurers are broadening coverage** without adequate rate consideration.
- Be aware of your current cyber risks across the enterprise – **Cyber Security is a business issue, not an IT topic.**

Question & Answers