RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: GRC-F02

DEBUNKING MYTHS FOR CYBER INSURANCE

Robert Jones

Global Head of Financial Lines Specialty Claims
AIG

Garin Pace

Cyber Product Leader
AIG
@Garin_Pace

Introduction – What Is Cyber Insurance?

What people think about cyber insurance:

- It only responds to data breaches
- It's only for malicious acts (attacks)
- It has stringent requirements, and requires compliance for coverage
- It's an admission of failure

The reality of cyber insurance:

- It can also respond to other failures of computer security, including business interruption loss, data restoration costs, and extortion threats
- It can cover accidental disclosure of confidential information, as well as systems failures
- Most policies do not have audit requirements, or require the insured to warrant a security posture
- You buy fire insurance, right?

AIG

Today’s Goal: Debunk common myths and help you to better use cyber insurance to improve your risk management strategy

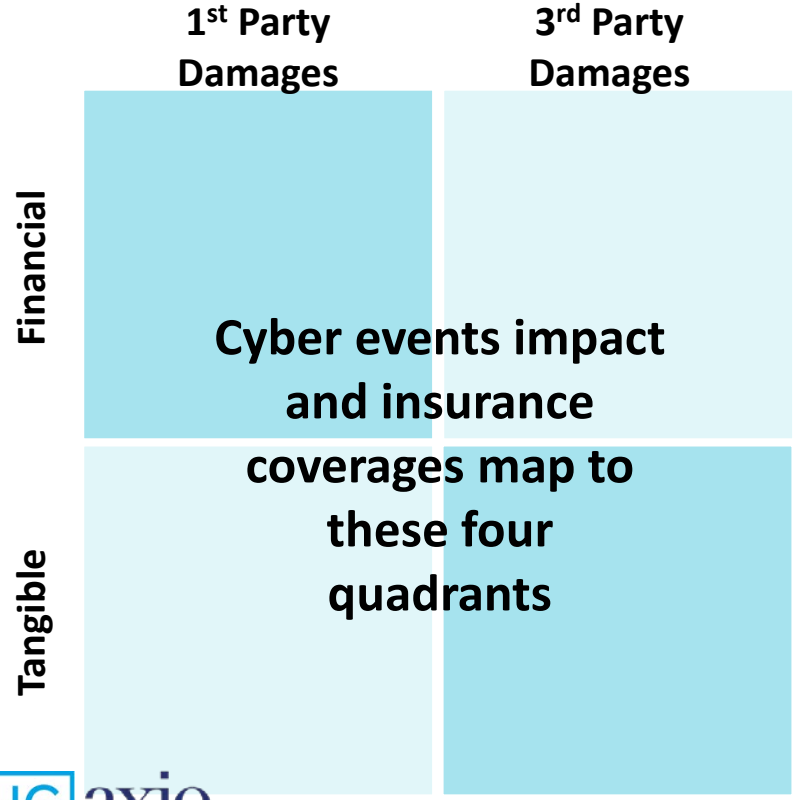
So, What Is Cyber Insurance REALLY?

Cyber insurance is an entire collection of insurance products.

THEN	NOW
• Addressed gaps in property and general liability policies (losses where there is no bodily injury or property damage) • Insurance products were sold as specific products responding to unauthorized access/use, DoS, etc.	• Cyber perils have many impacts: data loss, business interruption, liability, theft of money or fraudulent inducement, bodily injury, or even loss of real property • Insurance products and traditional coverages are being amended to respond to the new paradigm

AIG

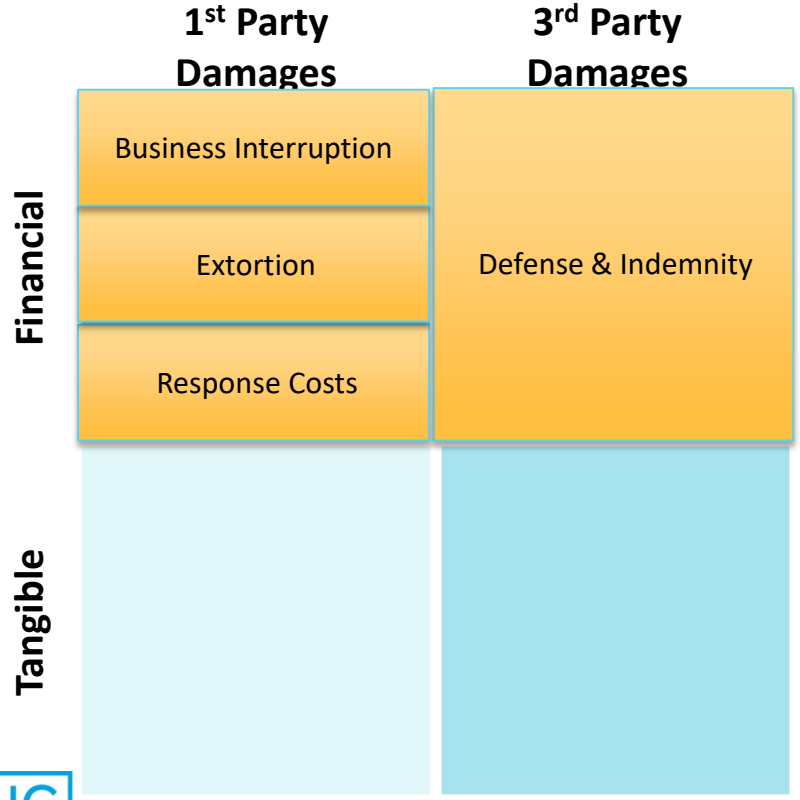
Cyber Impact Framework



- The Cyber Impact Framework – a tool created by AIG's partner axio – demonstrates the full spectrum of cyber risk
- It's useful for both conceptualizing the impacts of a cyber event, and mapping them to insurance coverage

AIG axio

The First Cyber Insurance Products



- The first cyber insurance products were (and many of those branded as such today still are) a collection of coverages offered a la carte
- Half of our buyers didn't even purchase business interruption until a few years ago

The First Cyber Insurance Products

The first cyber insurance products respond well to data breaches and other financial impacts where there was no tangible damage, but have important limitations:

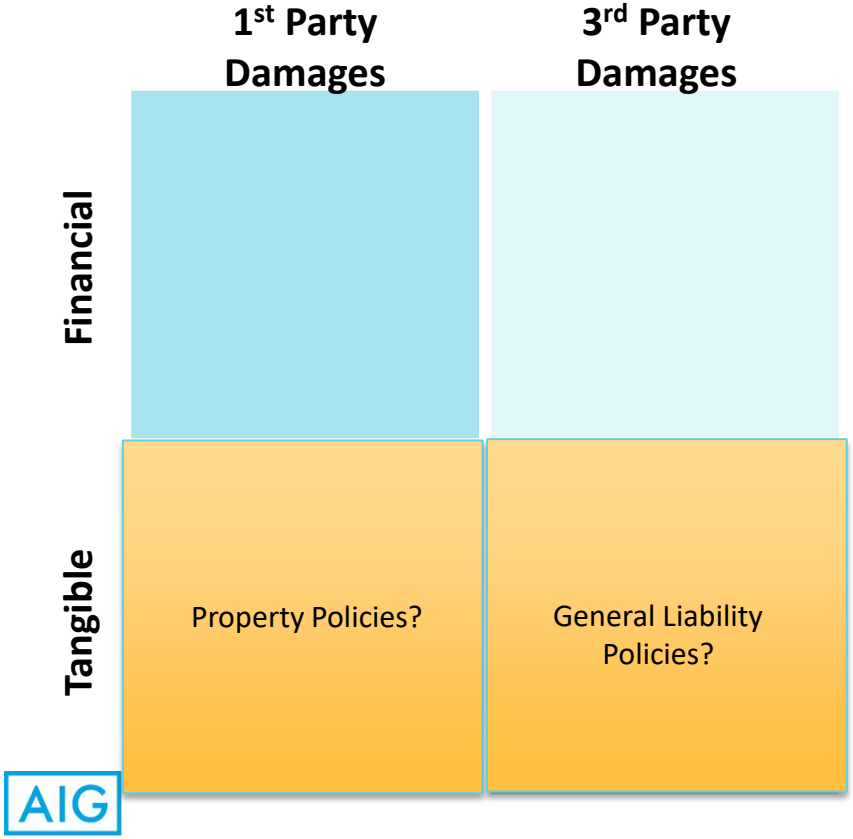
- They are typically subject to an exclusion for bodily injury or (tangible) property damage
- They typically do not cover theft of monies/securities
- They almost never cover the loss of intellectual property on a first-party basis

Evolution Of Cyber Insurance Products

Some early limitations of cyber insurance have mostly disappeared as both the products themselves and the insurers have matured:

- Exclusions for “known shortcomings of security”, including a requirement to patch, have diminished
- Insurers understand that “just patch” is an oversimplification; coverage is available even for organizations with end of life software
- Coverage for the most in demand costs – legal advice, forensics, and notification and monitoring costs – is typically not limited to smaller amounts than the policy limit

Cyber-Physical Loss And Silent Cyber



- "All risk" property and general liability policies have typically covered loss of tangible property and liability for property loss/bodily injury, respectively, even if arising out a cyber incident
- This is referred to as "silent cyber" given the policies do not explicitly provide coverage for cyber incidents

AIG

Cyber Physical Loss and Silent Cyber

How property and general liability policies address both physical cyber losses and financial losses is changing:

- Some insurers don't feel they have the expertise and/or appetite for cyber risk, and are **excluding** typically covered losses arising out of cyber incidents
- In contrast, some insurers are **expanding** coverage; for example, some property carriers are covering corruption of data even where there is no tangible property damage
- Even where coverage positions are not changing, more insurers are writing in affirmative coverage (no longer "silent"); insurance regulators desire certainty

AIG

Other Cyber Losses And Insurance Products

	Cyber	Property	General Liability	Crime	Directors & Officers
Theft of funds (monies/securities) via cyber means	X	X	X	✓	X
Coverage for shareholder actions following a cyber incident	X	X	X	X	✓

AIG

Other Cyber Losses And Insurance Products

- Other insurance policies **may** provide coverage for certain situations
- Kidnap, Ransom, and Extortion policies
  - May cover the cost of investigating ransomware or other cyber extortion, the demand itself, and any business interruption
  - The market was adversely impacted by ransomware, and most carriers are either now excluding coverage or changing the structure of coverage
- Errors and Omissions/Professional Liability policies
  - May provide defense and indemnity for claims brought by third parties alleging negligence with respect to a cyber incident
  - Example: legal malpractice policies may cover client suits, but typically do not cover first-party costs (investigation, notification, etc.)

AIG

CHECK-IN Q&A

(don’t worry – we’ll do Q&A at the end too)

LOSS EXAMPLES

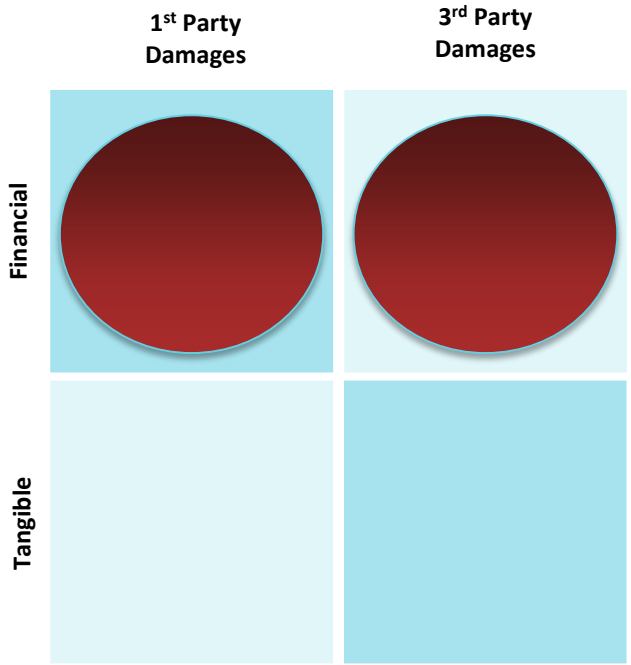
Hospital Data Breach

What happened?

- A hospital was notified by a third-party of a potential data breach
- Upon investigation, they confirmed the exposure of over 40K protected health information records, in violation of HIPAA

What difference did insurance make?

- AIG reimbursed the insured $1.24M in costs, including forensic investigation, legal advice, notification and identity monitoring, and regulatory fines



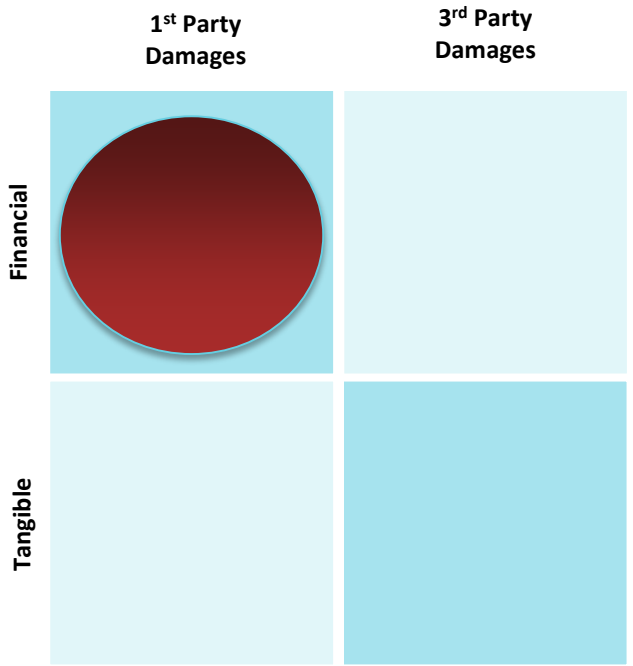
Law Firm Data Deletion

What happened?

- A disgruntled employee deleted organizational data – including firm intellectual property – from information systems and backups

What difference did insurance make?

- AIG reimbursed the insured $300K for the cost of re-creating/restoring the data



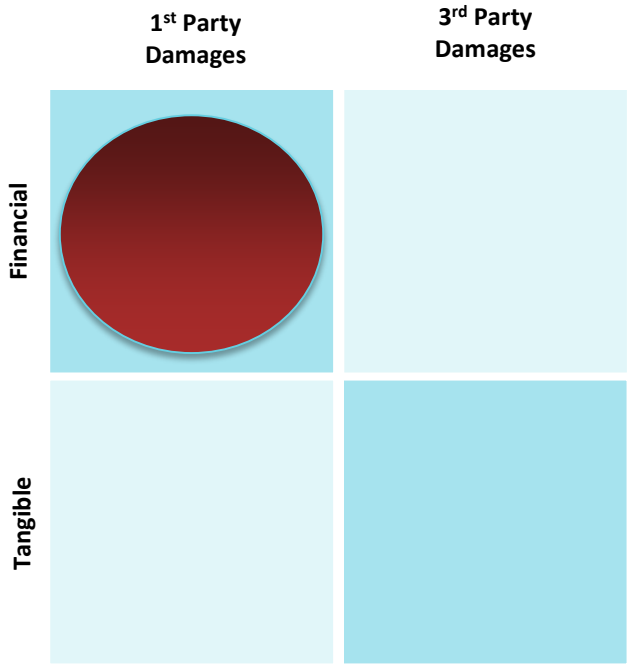
Cyber Extortion

What happened?

- An extortionist contacted an organization and provided evidence of both intrusion and exfiltration of data
- They threatened to make sensitive data public unless a ransom of $7M in BTC was paid

What difference did insurance make?

- AIG reimbursed the insured the cost of the forensic investigation, legal advice, and public relations
- Insurance covers the ransom, but AIG supported the insured's desire to refuse the ransom



AIG

INSURANCE AS A RISK MANAGEMENT TOOL

Cyber Risk Management

In the traditional approach to cyber risk management:

- IT groups were responsible for managing cyber risk; not recognized as an enterprise issue
- Risk management included risk mitigation, investment, risk acceptance (but very little, if any, risk transfer)
- Cyber risk was largely thought of as, and treated as, a technology problem

Cyber Risk Management

Cyber Risk Management Today:

- Enterprise issue
- Boards are concerned
- Social engineering and other “human” attacks a large part of cyber security
- Attackers generally target vulnerabilities, not organizations; collateral damage is significant
- “Not if, but when” – requires a comprehensive cyber risk strategy

AIG

Insurance's Part In Your Cyber Risk Strategy

Insurance is another cyber control, but with some unique properties:

- Unlike advanced controls – which tend to apply to specific scenarios – cyber insurance's benefit applies to most scenarios/costs
- Increasing cyber capabilities typically costs successively more, but cyber insurance generally decreases in cost with cyber maturity

Cyber insurance is **not** a replacement for a cyber risk program:

- Cyber insurance is often prohibitively expensive when an organization doesn't do the basics
- It also doesn't cover all loss types

AIG

Insurance's Part In Your Cyber Risk Strategy

In addition to the risk transfer, cyber insurance also provides other benefits both before and after a loss:

- Expertise in incident management and access to professionals
- Feedback, benchmarking, and trend analysis: claims statistics and common causes of loss help clients understand and mitigate the risk
- Risk quantification: cyber loss models are maturing and insurers are increasingly sharing model results with clients, both during underwriting and throughout the life of the policy

Insurance's Part In Your Cyber Risk Strategy

Cyber insurance continues to evolve:

- Insurers are partnering with information security vendors to promote best practices, give clients credit for hardening their environments, and bring objective data to bear
- By combining integration with technology products and model sophistication, 'continuous underwriting' and dynamic pricing become possible
- Coverage continues to evolve: more coverage for third party failures, more covered types of loss (reputation damage)

Correcting Other Myths & Misconceptions

- Insurers will cover ransomware; coverage exists for investigation costs, and the ransom payment (if necessary)
- Most cyber insurance policies cover both accidental and intentional acts by employees (executive leadership excepted)
- Cyber insurance **does** pay; insurers typically can't talk about the success stories – only the disagreements between insurers and insureds make the news; these are not representative
- Policies themselves are just like any other control, they must be tuned; talk with your insurer about expectations

AIG

Apply What You Have Learned

Next Steps:

- Talk to your Risk Manager (or whoever manages your company's risk program and insurance purchasing)
  - Get on the same page regarding your company's cyber risk profile
  - Review what coverage your existing policies afford your company

If you're taking more risk than you'd like, or if you're not sure if you are:

- Ask your broker how much experience they have placing cyber insurance
  - If they don't have a lot of experience, they may need to hire a "wholesaler" (an expert), or you may need to use a specialty broker for this placement
- Get a quote which covers the risks you identified; if you don't agree with the price, ask the insurer to share their rationale

AIG

Conclusion

- Cyber risk is a constantly evolving threat with potentially critical impact
- Like other severe perils, insurance can help to protect a company from catastrophe
- Cyber insurance is not a singular insurance product, but a collection of policies; depending on your threat profile and risk appetite, your needs will differ
- Insurers offer value in addition to pure risk transfer, including expertise in handling cyber incidents and ensuing litigation, and information on both threats and risk mitigation

AIG

American International Group, Inc. (AIG) is a leading global insurance organization. Founded in 1919, today AIG member companies provide a wide range of property casualty insurance, life insurance, retirement products, and other financial services to customers in more than 80 countries and jurisdictions. These diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance www.twitter.com/AIGinsurance | LinkedIn: www.linkedin.com/company/aig.

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.