

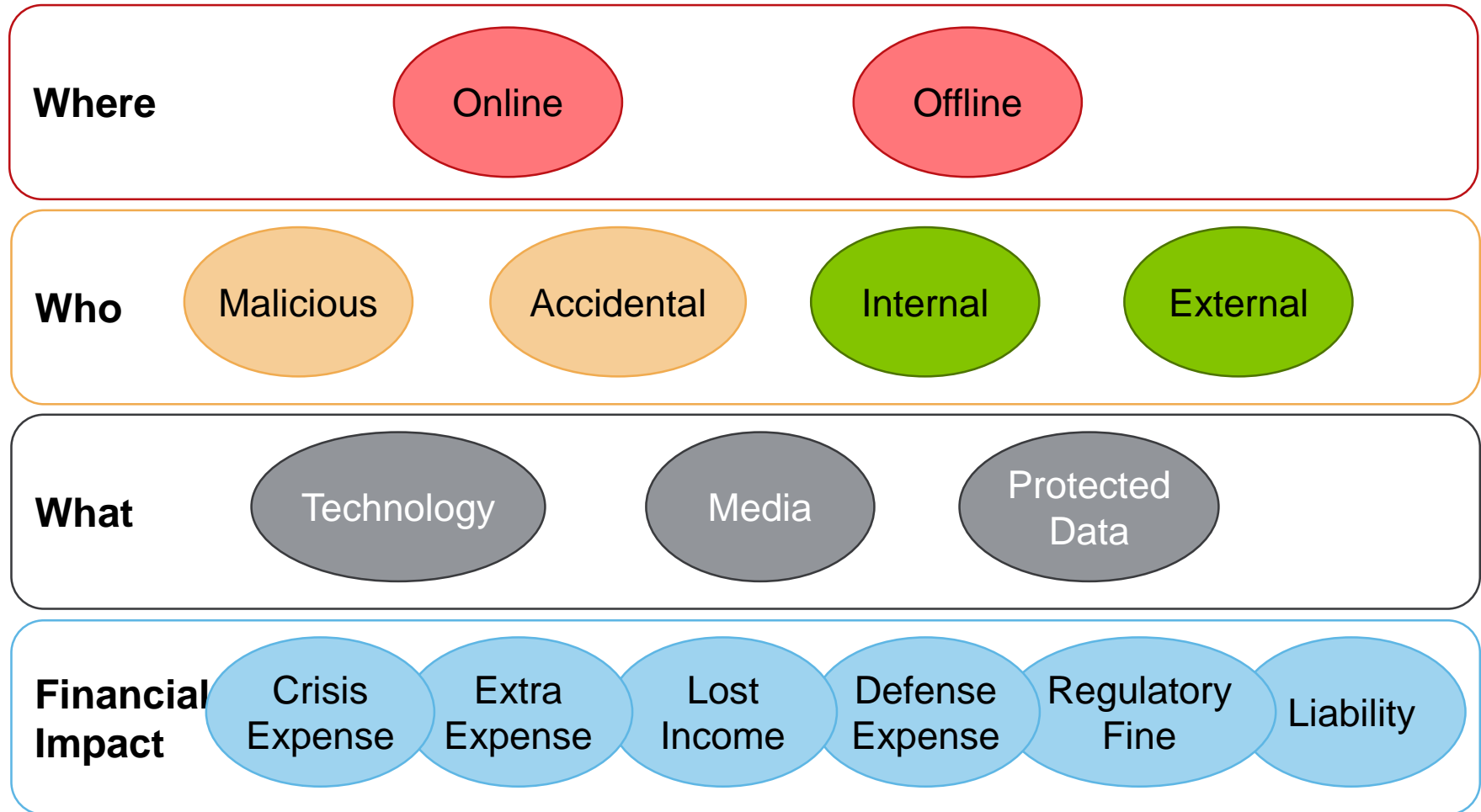


Cyber, The Fast-Moving Target

Presentation Date: September 22, 2016

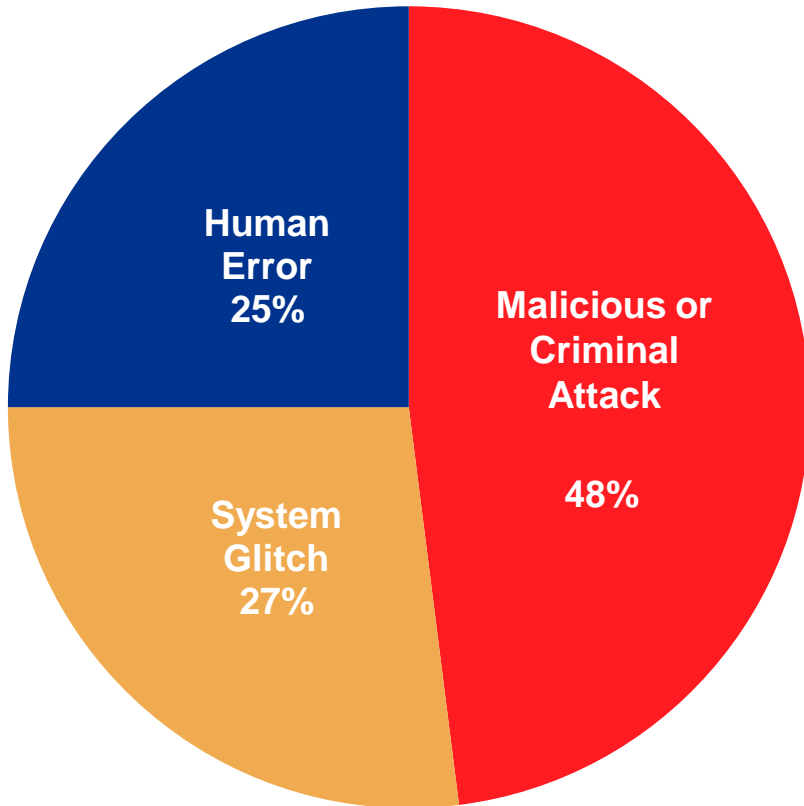
Financial Services Group
Professional Risk Solutions
Nolan Wilson | 305.961.6001 | nolan.wilson@aon.com

What Is Cyber?

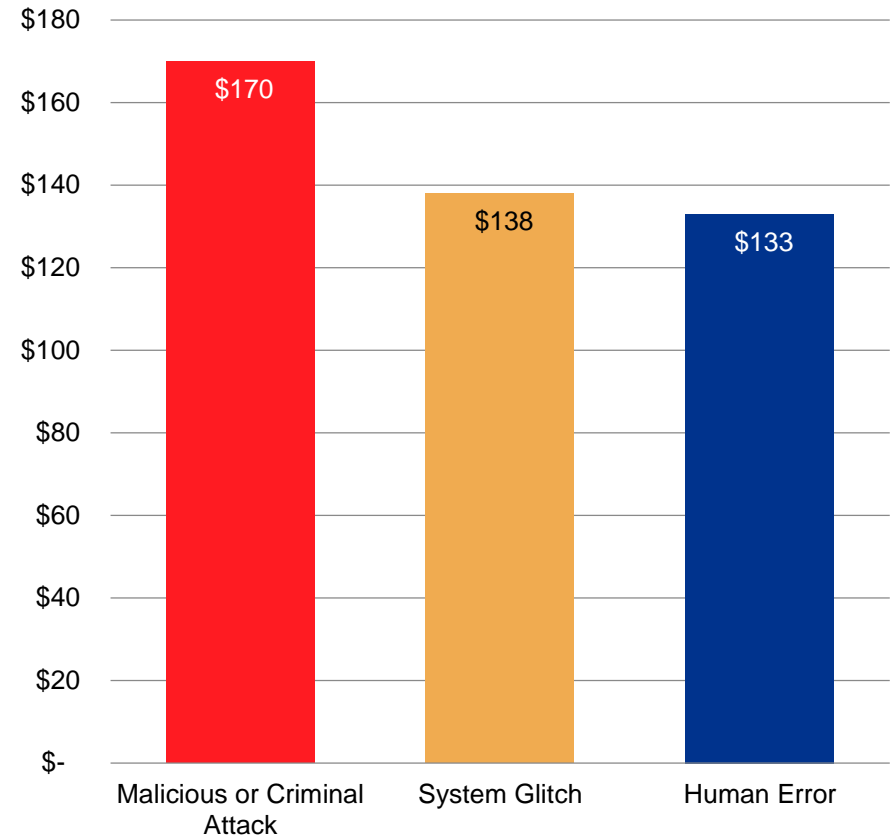


Root Causes of a Data Breach – Ponemon

Distribution of Root Cause of Data Breach



Per Capita Cost for Root Causes of the Data Breach



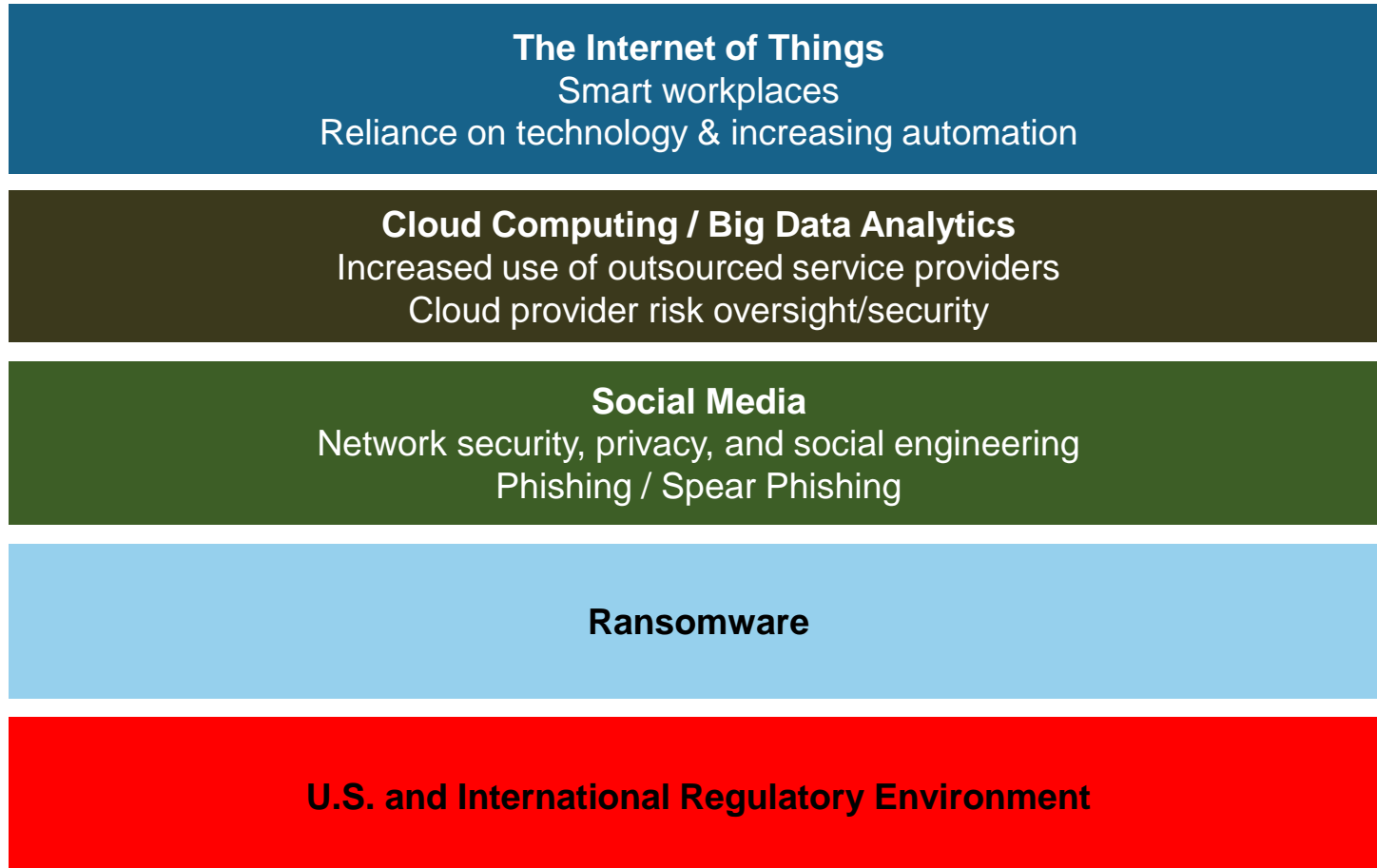
Source: Ponemon Institute 2016 Cost of Data Breach Study

Average Cost of a Data Breach – Ponemon Report

U.S Data	Average Cost per U.S Data Breach Event	Average Cost per Compromised Record	% Caused by Malicious Attacks
2016	\$7.01M	\$221	48%
2015	\$6.53M	\$217	49%
2014	\$5.85M	\$201	44%
2013	\$5.4M	\$188	41%
2012	\$5.5M	\$194	37%
2011	\$7.2M	\$214	31%
2010	\$6.8M	\$204	24%
2009	\$6.7M	\$202	12%
2008	\$6.3M	\$197	Not tracked
2007	\$4.8M	\$182	Not tracked

- May 2015: Ponemon Institute’s 2016 Global Cost of a Data Breach
- Analyzes cost of data breach incident response for companies in 10 countries
- Does NOT include Legal Defense, PCI-DSS Assessments, Regulatory Fines, or Damages
 - A portion of the “cost” in this study = abnormal churn post-breach = uninsurable in Cyber policies
 - Study excludes data breaches in excess of 100,000 records

2016 Cyber Exposure Trends



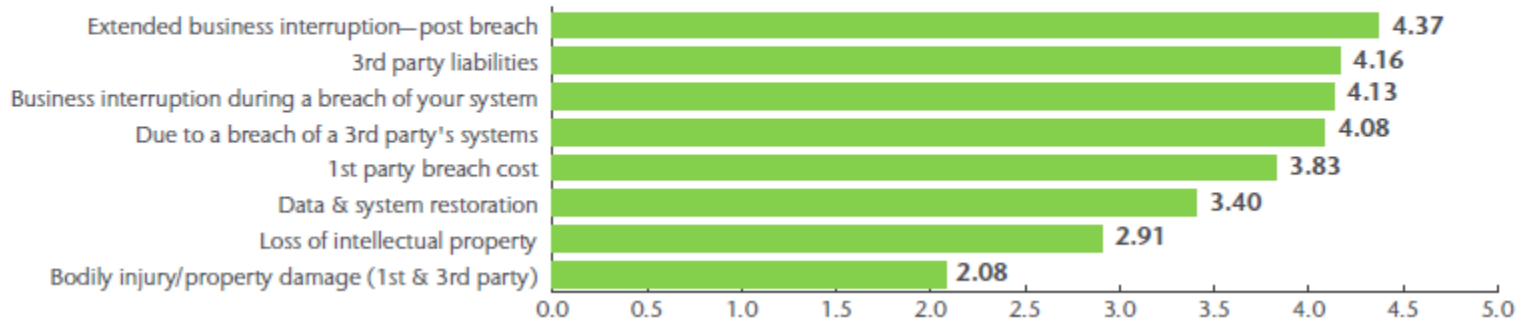
2016 Aon Cyber Benchmarking Survey

Topics	Data Holders	Product Risk	Critical Infrastructure	Transportation	Heavy Industry
Top Cyber Risk Concern	Post Breach Business Interruption	Business Interruption	Business Interruption	Business Interruption	Business Interruption
Lowest Cyber Risk Concern	Bodily Injury/Property Damage	Bodily Injury/Property Damage	Data & System Restoration	Loss of IP	Bodily Injury/Property Damage
Use of Risk Assessment to inform Coverage/limits	51%	75%	59%	70%	56%
Rationale for buying cover	Board Due Diligence (80%)	Balance Sheet Protection (58%)	Balance Sheet Protection (71%)	Balance Sheet Protection (64%)	Board Due Diligence (56%)
Who is buying	70%	17%	29%	33%	33%
Limits (m)	USD 10-25	USD 10-25	>USD 100	USD 10-25	USD 10-25
Budgeted for Cyber Cover	74%	31%	41%	9%	33%

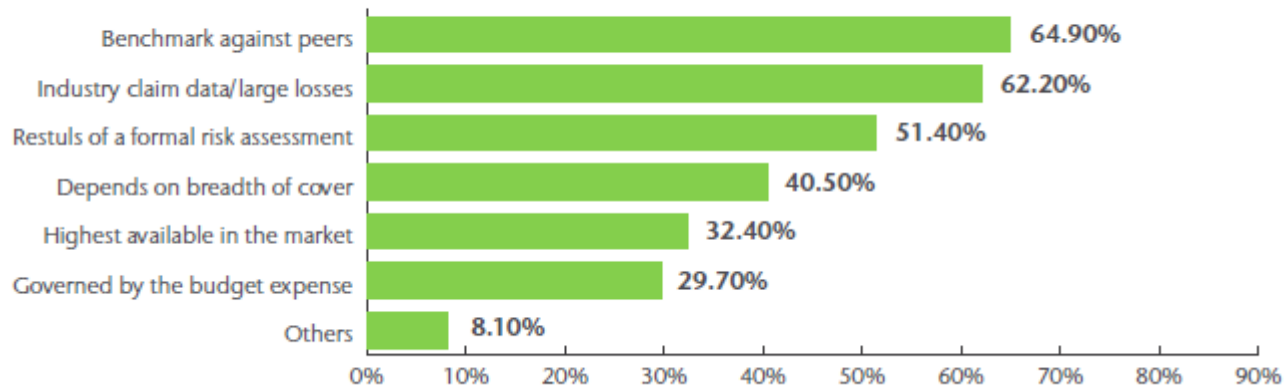
Source: 2016 Aon Captive Cyber Benchmarking Survey by Industry
 Cyber—The Fast Moving Target: Benchmarking views and attitudes by industry: <http://www.aon.com/risk-services/cyber.jsp>

2016 Aon Cyber Benchmarking Survey

Which elements in cyber risk give you the greatest cause for concern?



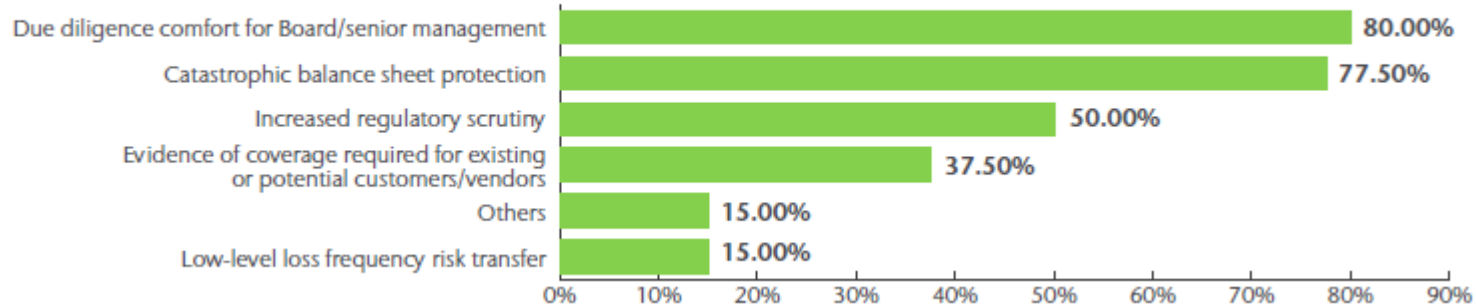
When deciding on total limits to insure, which factors influence the decision?



Source: 2016 Aon Captive Cyber Benchmarking Survey by Industry
Cyber—The Fast Moving Target: Benchmarking views and attitudes by industry: <http://www.aon.com/risk-services/cyber.jsp>

2016 Aon Cyber Benchmarking Survey

What are your main reasons for purchasing or considering cyber insurance?



Do you currently buy cyber insurance?



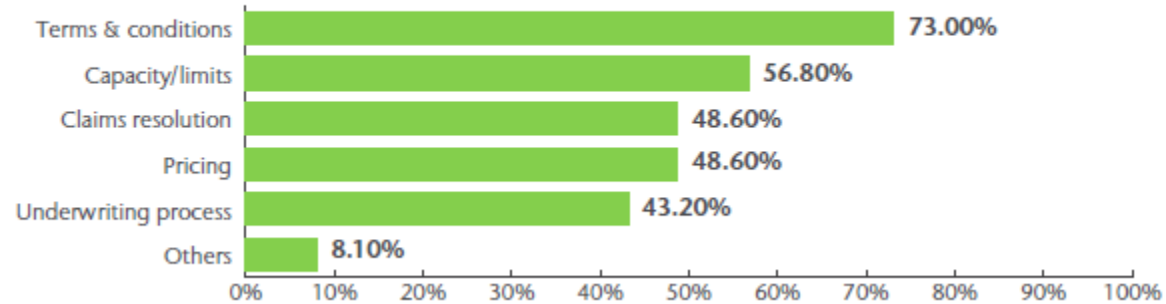
Is the expense for cyber insurance currently in budget?



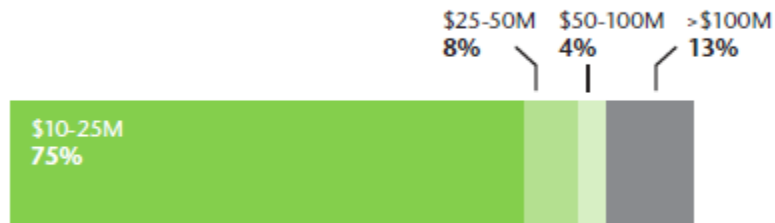
Source: 2016 Aon Captive Cyber Benchmarking Survey by Industry
Cyber—The Fast Moving Target: Benchmarking views and attitudes by industry: <http://www.aon.com/risk-services/cyber.jsp>

2016 Aon Cyber Benchmarking Survey

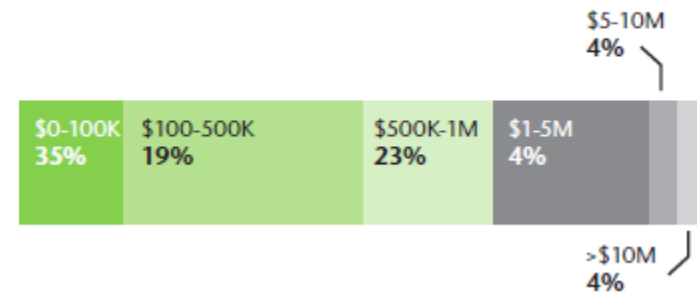
What do you perceive as the greatest issues in the cyber risk market place?



Limits



Retention levels

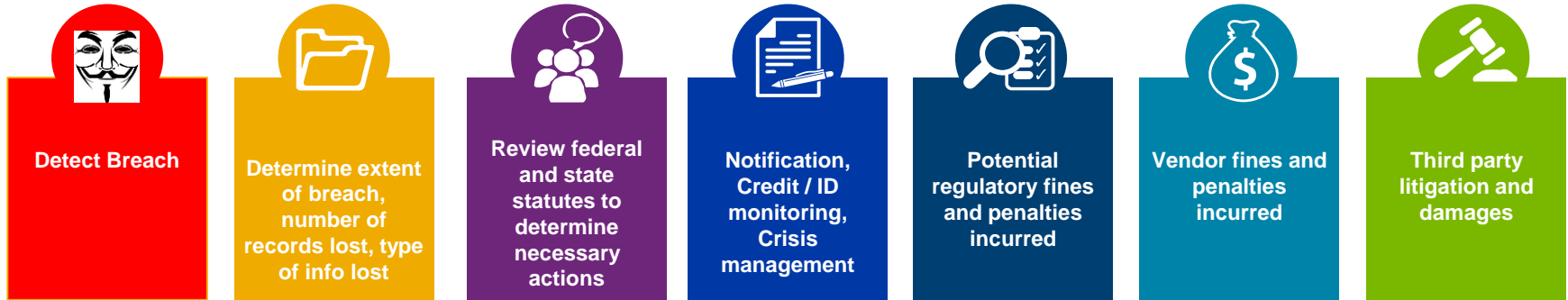


Source: 2016 Aon Captive Cyber Benchmarking Survey by Industry
 Cyber—The Fast Moving Target: Benchmarking views and attitudes by industry: <http://www.aon.com/risk-services/cyber.jsp>

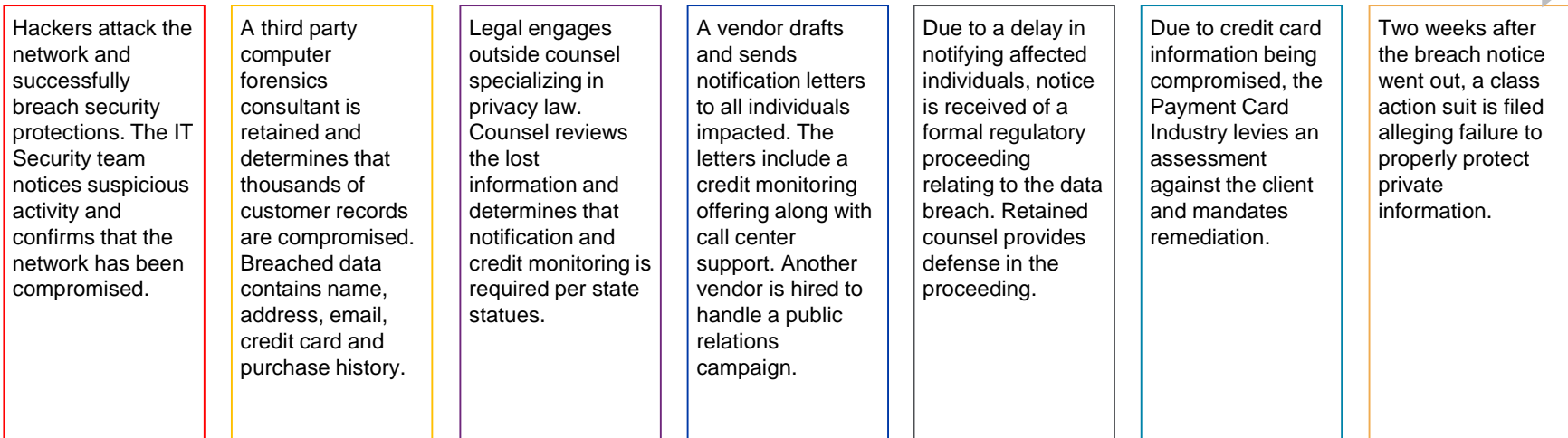
Financial Institutions – Cyber Exposures

- Subject to regulatory statutes such as Gramm-Leach Bliley Act (GLBA) and oversight from the Federal Financial Institutions Examination Council (FFIEC) and Financial Industry Regulatory Authority (FINRA)
- IT infrastructure interruption
- Recent targeted attacks (State sponsored and rise in social engineering related attacks) (spear fishing)
- Significant amounts of credit card information, bank account information, driver's licenses, credit information, etc
 - Personally identifiable information
- Reputational harm (trust)
- Limited defense resources

Loss Statistics: Start with a Privacy Breach Example



How it plays out...



Data Breach Claim Example – Financial Institutions

Firm:	RBS WorldPay
Country(ies):	Data breach affected firm based in the US (Georgia); breach affected ATMs in more than 280 cities worldwide, including cities in the US and Hong Kong; hackers involved were located in Russia and Estonia.
Year of Breach:	2008
Amount(s) at Issue:	More than US\$9 million was stolen from ATMs
Approximate Records	1.5 million
Sources:	Court Docket, Irwin v. RBS WorldPay, Inc., Case No. 1:09-cv-00033, June 22, 2010 (last accessed, Aug. 11, 2015); InformationWeek, Nov. 23, 2009; Wall Street Journal, Nov. 11, 2009; Computer Weekly, May 26, 2009; The Herald, Feb. 9, 2009; Digital Transactions, Feb. 4, 2009; New York Post, Feb. 4, 2009; Credit Union Times, Jan. 21, 2009; Privacy Rights Clearinghouse, Dec. 29, 2008 (last accessed, Aug. 11, 2015).

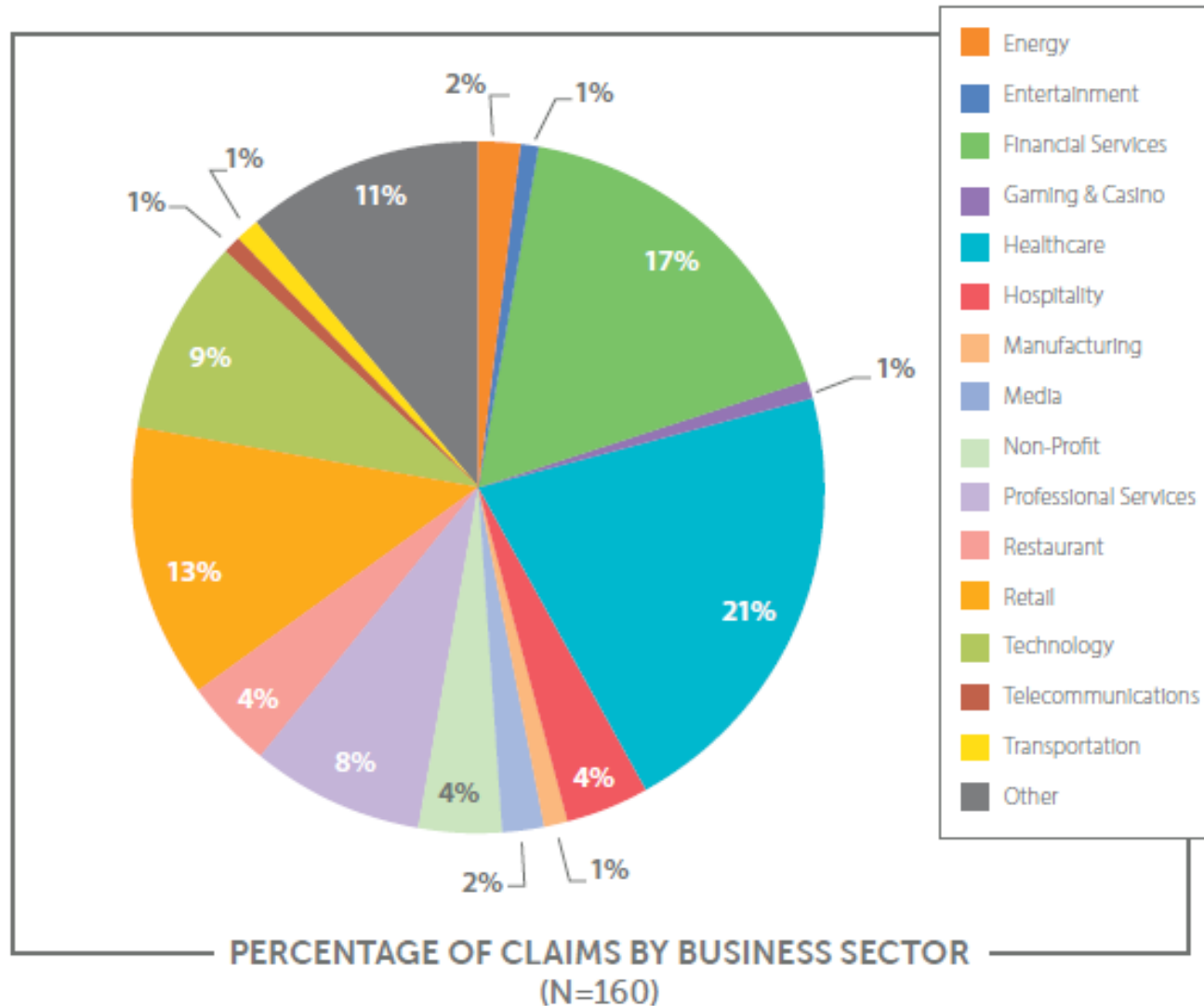
Summary:

In November 2008, hackers from locations outside of the US broke into the computer systems of RBS WorldPay Inc., the US payment processing arm of the Royal Bank of Scotland Group PLC (RBS). Over the course of no more than 12 hours, the hackers stole and cloned prepaid ATM cards which they reportedly used to steal more than \$9 million from 2,100 ATMs in 280 cities worldwide. The hackers were said to have developed a method by which they reverse engineered personal identification numbers associated with the prepaid cards from the encrypted data on the RBS WorldPay computer network. Experts speculated that, rather than cracking the encryption itself, it was more likely that the encryption had been defeated after the hackers found a way to grant themselves super-user privileges inside RBS WorldPay's Hardware Security Module. The data breach was detected by RBS WorldPay two days after the incident and was not publicly disclosed until December 2009. At the time of disclosure, RBS WorldPay acknowledged that the data of 1.5 million ATM cardholders had been compromised and 1.1 million Social Security numbers may have been compromised.

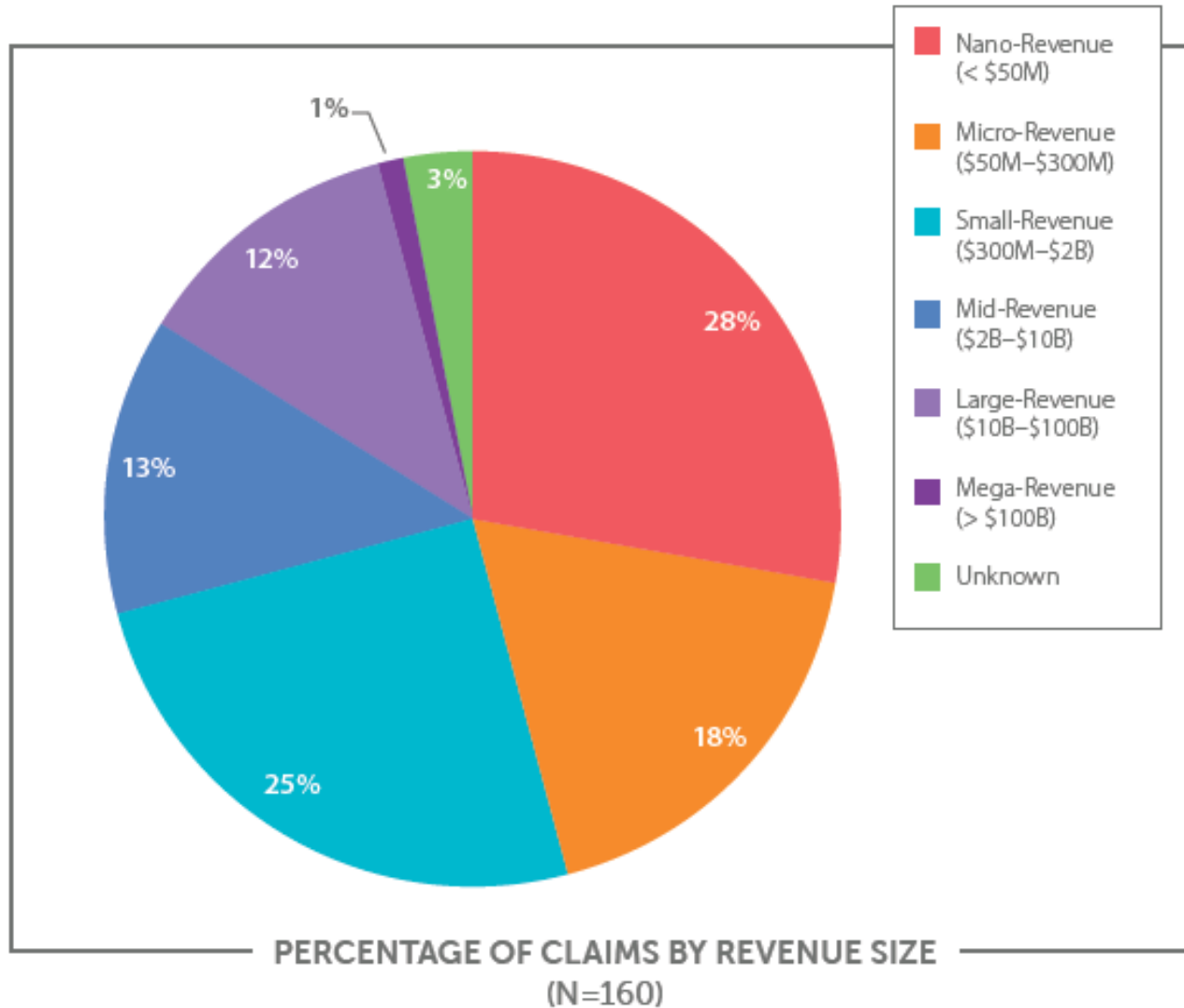
The US Justice Department indicted eight computer hackers from Russia and Eastern Europe who were allegedly part of the crime ring involved in the RBS WorldPay data breach. According to the indictment, the alleged hackers targeted prepaid ATM cards that companies issue employees for withdrawing their salaries. Once the hackers entered the systems, they increased the maximum allowed withdrawal and then tried to destroy data on the systems to cover up the break-in. The most serious charges in the 16-count grand jury indictment were against four conspirators and ranged from wire fraud to aggravated identity theft. Others faced lesser charges. In August 2012, the leader of the crime ring was sentenced to 2.5 years in federal prison. After the data breach, RBS WorldPay reimbursed customers for stolen funds and reportedly recalled and destroyed the prepaid cards involved in the hack. RBS also offered free credit report monitoring to the people whose Social Security numbers were potentially compromised. A security firm was hired by RBS WorldPay to determine how the incident occurred and to prevent such incidents from happening again.

In January 2009, a multi-million dollar class action lawsuit against RBS WorldPay was filed in federal court in Georgia, alleging the company failed to adequately protect customer data and claiming the delay in the disclosure to be negligent, in part because RBS WorldPay waited until after the holiday shopping season to make the disclosure. It is unclear from public sources whether the case was settled, but court records indicate the lawsuit was dismissed, by stipulation of the parties, in June 2010.

NetDiligence 2015 Claims Study – Claims by Industry



Net Diligence 2015 Claims Study – Claims by Company Size



Data Breach Claim Example – Financial Institutions (1 of 2)

Firm:	JPMorgan Chase
Industry:	Financial Services
Country(ies):	Data breach affected firm based in the US (New York); US federal and state regulators had been investigating the breach.
Year of Breach:	2014
Amount(s) at Issue:	Not applicable
Approximate Records Affected	76 million
Sources:	Law360, Jan. 14, 2015; New York Times, Dec. 22 and Oct. 8, 2014; The Atlantic, Oct. 3, 2014; Law360, Oct. 3, 2014; Wall Street Journal, Oct. 2, 2014; Tom's Guide: Tech for Real Life, Sept. 14, 2014; Fox News, Aug. 28, 2014; CNET, Aug. 28, 2014; Privacy Rights Clearinghouse, Aug. 28, 2014 (last accessed, Aug. 11, 2015).

Summary

In August 2014, it was disclosed that a cyber-attack on JPMorgan Chase & Co. (JPMorgan) compromised the personal information of about 76 million households in what was reported to be “the largest intrusion of an American bank to date” and “one of the most sweeping disclosed breaches of a financial institution.” The personal information accessed by hackers in the data breach included names, addresses, phone numbers and email addresses. Information on an additional 7 million small businesses was reportedly accessed as well. In September 2014, JPMorgan confirmed that the hackers were not able to access financial or bank account information, and explained that customer money was “safe.” The FBI and other federal authorities, including the National Security Agency as well as several state attorneys general, have all been investigating the data breach.

The attack went unnoticed during the summer of 2014, between mid-June and mid-August, when hackers repeatedly breached JPMorgan’s servers for around an hour at a time. JPMorgan discovered the hackers inside its systems in mid-August, after first finding that the same group of hackers had breached a website for a charitable race that the bank sponsored. The attack was said to have been caused by malicious computer code, known as malware. Hackers appear to have originally breached JPMorgan’s network via an employee’s personal computer. Experts surmised that the hackers spent a significant amount of time researching and studying the record system of the bank prior to attempting any kind of unauthorized access, and were able to modify records using high-level credentials in a way that was undetected. Later articles stated that the data accessed was related to JPMorgan’s marketing functions rather than its banking operations which made the data breach “less concerning,” though experts noted that the potential stolen information could be used to send phishing emails. In August 2014, hackers appeared to be targeting customers with such emails, though it was unclear if the incidents were related.

Data Breach Claim Example – Financial Institutions (2 of 2)

Firm:	JPMorgan Chase
Industry:	Financial Services
Country(ies):	Data breach affected firm based in the US (New York); US federal and state regulators had been investigating the breach.
Year of Breach:	2014
Approximate Records Affected	76 million

Summary Continued

In October 2014, it was reported that JPMorgan had not seen unusual levels of fraud since the attack, but had stated that customers would not be liable for any unauthorized transactions on their accounts. The bank reset the passwords of every technology employee and disabled accounts that may have been compromised. Since mid-August 2014 hundreds of employees across JPMorgan’s technology and cybersecurity teams had been working to examine data on servers compromised during the attack. A core team of around 20 JPMorgan employees oversaw the bank’s response to the cyber-attack, led by its chief operating officer, who sent a memo to employees in October 2014. The memo detailed the scope of the attacks, reminding employees to be “increasingly vigilant in the cyber world,” and to make sure they had “fortified” their own defenses, such as logging off workstations, changing passwords often and choosing passwords hard for others to guess. The memo also reiterated that employees could not use work email for personal use, should not open emails from anyone they did not know, and should only use “reliable software.” Because hackers gained access to more than 90 of JPMorgan’s servers, reports note that the bank needed to strip out and replace much of its internal IT infrastructure after the data breach, a process that experts estimated could take “months at the least.”

In December 2014, it was reported that the data breach at JPMorgan could have been avoided had the bank installed a simple security fix to an overlooked server in its vast network. While most large financial institutions use a two-factor authentication scheme, which requires a second one-time password to gain access to a protected system, JPMorgan’s security team had neglected to upgrade one of its network servers with the dual password scheme, leaving the bank vulnerable to intrusion. The oversight is now the focus of an internal review at JPMorgan seeking to identify other holes in the bank’s network.

Legal analysts have speculated that, as a result of the data breach, JPMorgan would likely face “a wave of class actions,” but have also acknowledged that the bank may have “an easier time skirting liability” than other institutions that have been subject to breaches given JPMorgan’s claim that the only data compromised was customers’ contact information.

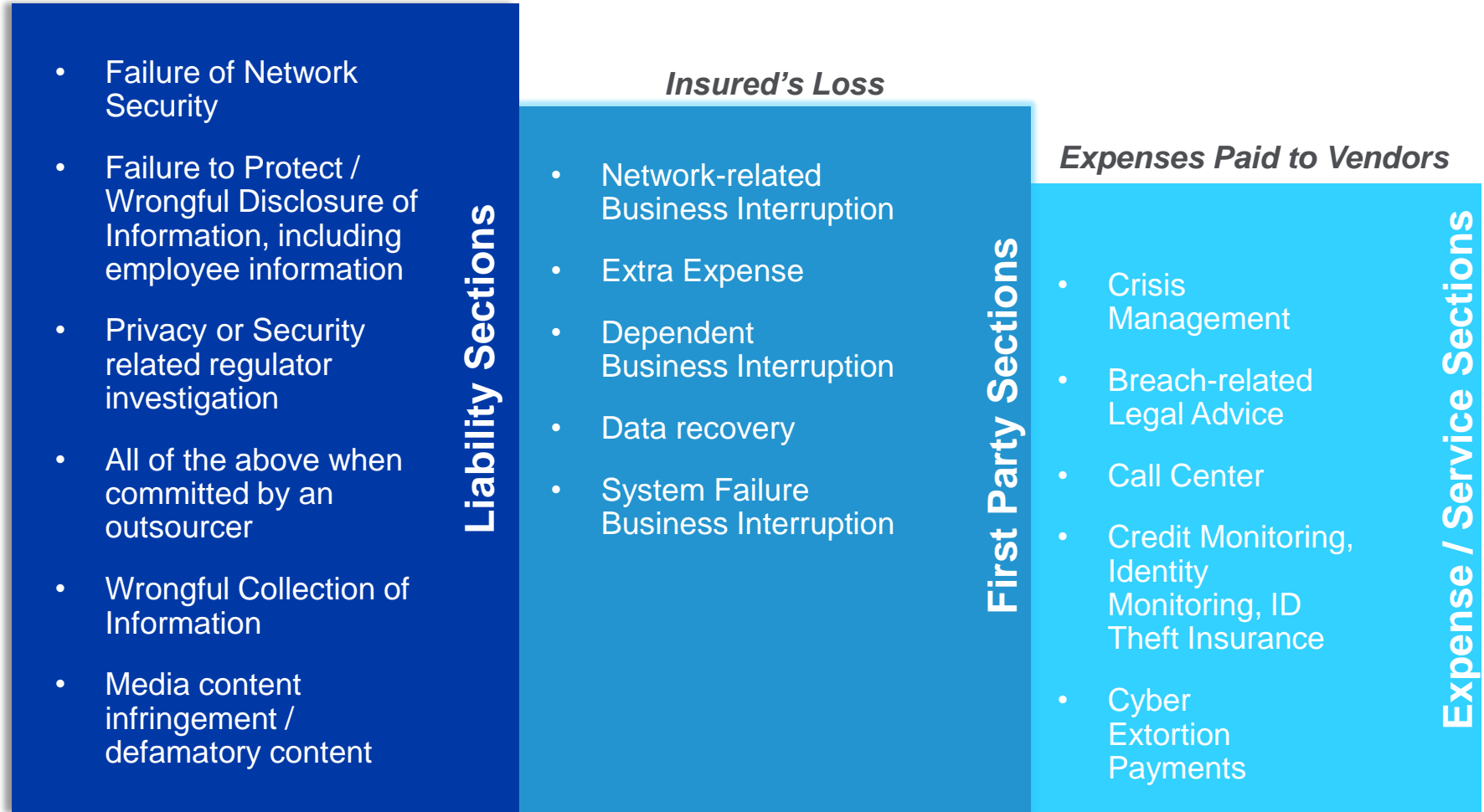
According to the press, in early December 2014, JPMorgan’s legal department sent an email to a number of its technology and cybersecurity employees reminding them not to “destroy or delete” any relevant documents about the data breach. Companies customarily send out such litigation “hold” notices when they receive subpoenas or requests for documents from regulators and law enforcement agencies. In January 2015, 15 state attorneys general sent JPMorgan a letter requesting greater detail about the data breach and how the bank planned to prevent another cyber-attack.

Financial Institutions – Cyber Claims Examples

Date Made Public	Incident
October 2, 2015	Schwab Retirement Plan Services Inc. (SRPS), notified customers of a data breach when a spreadsheet containing Social Security numbers, names, addresses, dates of birth, dates of termination, employment status, division code, marital status and account balance was accidentally emailed to a participant in another retirement plan serviced by SRPS
October 1, 2015	Experian announced a breach to their system affecting over 15 million T-Mobile customers. T-Mobile uses Experian to run credit checks on potential customers. Experian said the incident is "isolated" and is only limited to consumers who applied for T-Mobile USA services between Sept. 1, 2013, and Sept. 16, 2015. The information exposed to hackers includes names, addresses, social security numbers, dates of birth, and various identification numbers, including a passport, driver's license or military identification number, according to Experian, T-Mobile is offering 2 years free of identity theft monitoring services through Experian.
September 25, 2015	Blue Cross BlueShield of North Carolina notified customers of a data breach when they discovered two incidences that may have exposed personal information. The first incident occurred when a printing error resulted in members' billing invoice information printed on the back of other members' invoices. The information exposed here included names, addresses, internal BCBSNC account numbers, group numbers, coverage dates and premium amounts. The second incident occurred when payment letters included incorrect information and sent to the wrong members. This information included they type of health plan purchased, effective dates, health insurance marketplace identification numbers, payment amounts, telephone numbers and payment identification numbers.
September 25, 2015	<p>Excellus Blue Cross Blue Shield</p> <p>Excellus has revealed that in August the company discovered a breach to their system that may have started two years prior by hackers, gaining access to its customers' information.</p> <p>The information accessed included names, birth dates, Social Security numbers, mailing addresses, telephone numbers, claims and financial payment information, which included some credit card numbers. "Excellus spokesperson Cane confirmed in a phone call with WIRED that between 10 and 10.5 million customers had their data potentially accessed in the breach. Beyond just Excellus itself, the company says that even some of its insurance partners within the Blue Cross Blue Shield network may be affected, accounting for about 3.5 million of those victims. Everyone affected will receive a letter from Excellus, along with two years of free credit monitoring from the company."</p>

Scope of Cyber Insurance Coverage Available In The Marketplace

Defense Costs + Damages + Regulator Fines



Cyber Policies – Consistently Inconsistent

Consider:

- What is my primary policy first party coverage trigger?
- Are all coverages subject to a retroactive date?
- How many retentions apply to my policy?
- What is the definition of computer system?
- Does the policy include regulatory fines & penalties and PCI assessments?
 - Are they sublimited or are full limits available?
- Notable non-standard exclusions:
 - Unencrypted device exclusions
 - Failure to maintain minimum security standards
 - Unsupported technology exclusion
 - Technology “wear and tear” exclusions
- Is there appropriate coverage for:
 - System failure – is coverage available?
 - Business / network interruption – is there an hourly sublimit?
 - Cyber terrorism – is there affirmative coverage or silence?

First Party Coverage Elements – Triggered By A Breach

- **Data Breach Response and Crisis Management Coverage:** Reimbursement for the insured's costs to respond to a data privacy or security incident. Policies are triggered either by the discovery of such an event, or a statutory obligation to notify customers of such an event. Covered expenses can include:
 - Legal expenses
 - Computer forensics expenses
 - Public relations firm expenses and related advertising to restore your reputation
 - Notification to consumers
 - Consumer credit monitoring services
- **Personally identifiable information** (PII), or Sensitive Personal Information (SPI), as used in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context
 - NIST define personally identifiable information as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."
- **Network Extortion Coverage:** *Triggered by a threat to cause a security failure or privacy breach.* Reimburses the insured for expenses incurred in the investigation of a threat and any extortion payments made to prevent or resolve the threat. Payments are generally subject to full discretion by insurer.

*This is a summary only, refer to actual policy language for coverage afforded in the policy

First Party Coverage Elements – Triggered By A Breach

- **Business Interruption:** Reimburses the insured for actual lost net income and extra expense incurred when the insured's computer system is interrupted or suspended due to a failure of network security. In addition to a dollar amount retention, a waiting period retention of between 6 to 12 hours applies.
- **Dependent Business Interruption:** Reimburses the insured for actual lost net income and extra expense incurred when the insured's Service Provider's computer system is interrupted or suspended due to a failure of network security.
- **Data Recovery:** Reimburses the insured for costs incurred to restore or recollect intangible, non-physical assets (software or data) that are corrupted, destroyed or deleted due to a covered computer network security failure.
- **System Failure:** Available upon request which provides limited coverage for business interruption due to an unintentional or unplanned system failure not caused by a failure of network security

*This is a summary only, refer to actual policy language for coverage afforded in the policy

Third Party Coverage Elements – Triggered By A Claim

- **Security and Privacy Liability:** Coverage for defense costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or wrongful disclosure of confidential information, unauthorized access, unauthorized use, denial of service attack or transmission of a computer virus.
- **Privacy Regulatory Defense, Awards and Fines:** Coverage for defense costs for proceedings brought by a governmental agency in connection with a failure to protect private information and / or a failure of network security. Coverage may be sub-limited and may include (depending on insurer) coverage for fines and penalties to the extent insurable by law.
- **Payment Card Industry (PCI) Data Security Standards (DSS) Fines and Assessments:** Coverage for defense costs for investigations brought by the Payment Card Industry in connection with a failure to protect private information and / or a failure of network security that may have resulted from being non-compliant with PCI DSS.
- **Media Liability:** Coverage for defense costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright infringement, trademark infringement, or invasion of privacy. The scope of covered media is variable and can range from the insured's website only to all content in any medium.

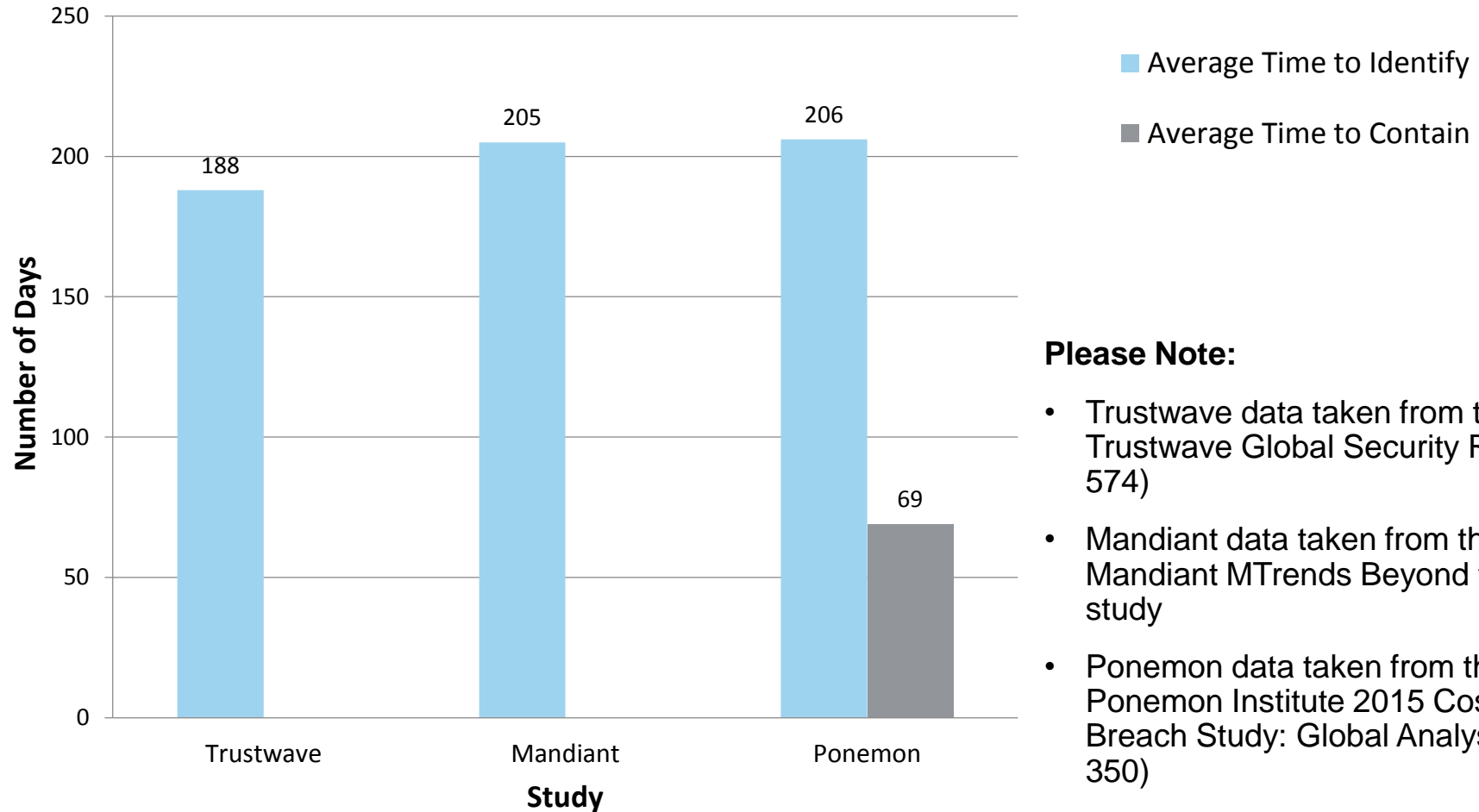
*This is a summary only, refer to actual policy language for coverage afforded in the policy

Sample First Party Incident Resources

Most insurers offer a list of panel vendors – examples include:

Legal	<ul style="list-style-type: none"> • Lewis Brisbois • Information Law Group • Edwards Widman Palmer LLP • Baker & Hostetler LLP • Marshall Dennehy Warner Coleman & Goggin 	<ul style="list-style-type: none"> • Nelson Mullins Riley & Scarborough • Wilson Elser • McDonald Hopkins LLC • Jackson Lewis LLP • Lewis Brisbois Bisgaard & Smith LLP • Alston & Bird
Data Breach Coach	<ul style="list-style-type: none"> • Wiggin & Dana, LLP • Lewis Brisbois, Bisgaard & Smith, LLP 	<ul style="list-style-type: none"> • Nelson Levine de Luca & Hamilton • Baker Hostetler
Forensics	<ul style="list-style-type: none"> • Kroll Ontrack, Inc. • Stroz Friedberg • Verizon • Navigant Consulting, Inc. • Intelligent Discovery Solutions 	<ul style="list-style-type: none"> • Net Diligence • Digital Discovery • Accuvant • PWC • Trustwave
Notification & Call Center	<ul style="list-style-type: none"> • Debix / All Clear ID • Immersion • ID Experts 	<ul style="list-style-type: none"> • Kroll Background America, Inc. • Epiq Corporate Services, Inc. • Intelligent Business Concepts, Inc.
Credit Monitoring	<ul style="list-style-type: none"> • ID Experts • Kroll Background America, Inc. • All Clear ID • Experian 	<ul style="list-style-type: none"> • TransUnion • Equifax • Info Armour
Crisis Management	<ul style="list-style-type: none"> • Fleishman Hillard 	

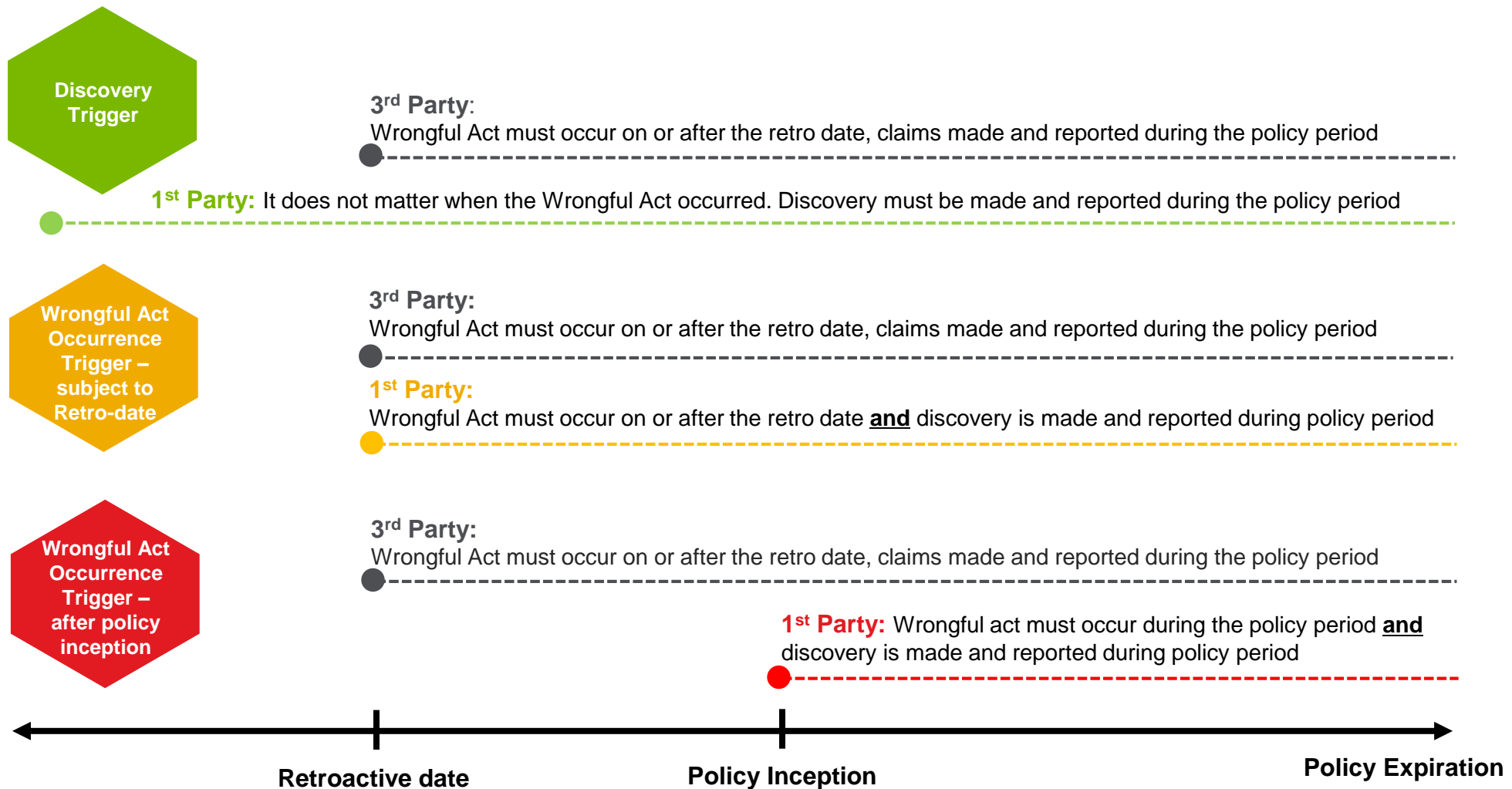
Average Time to Identify a Data Breach



Please Note:

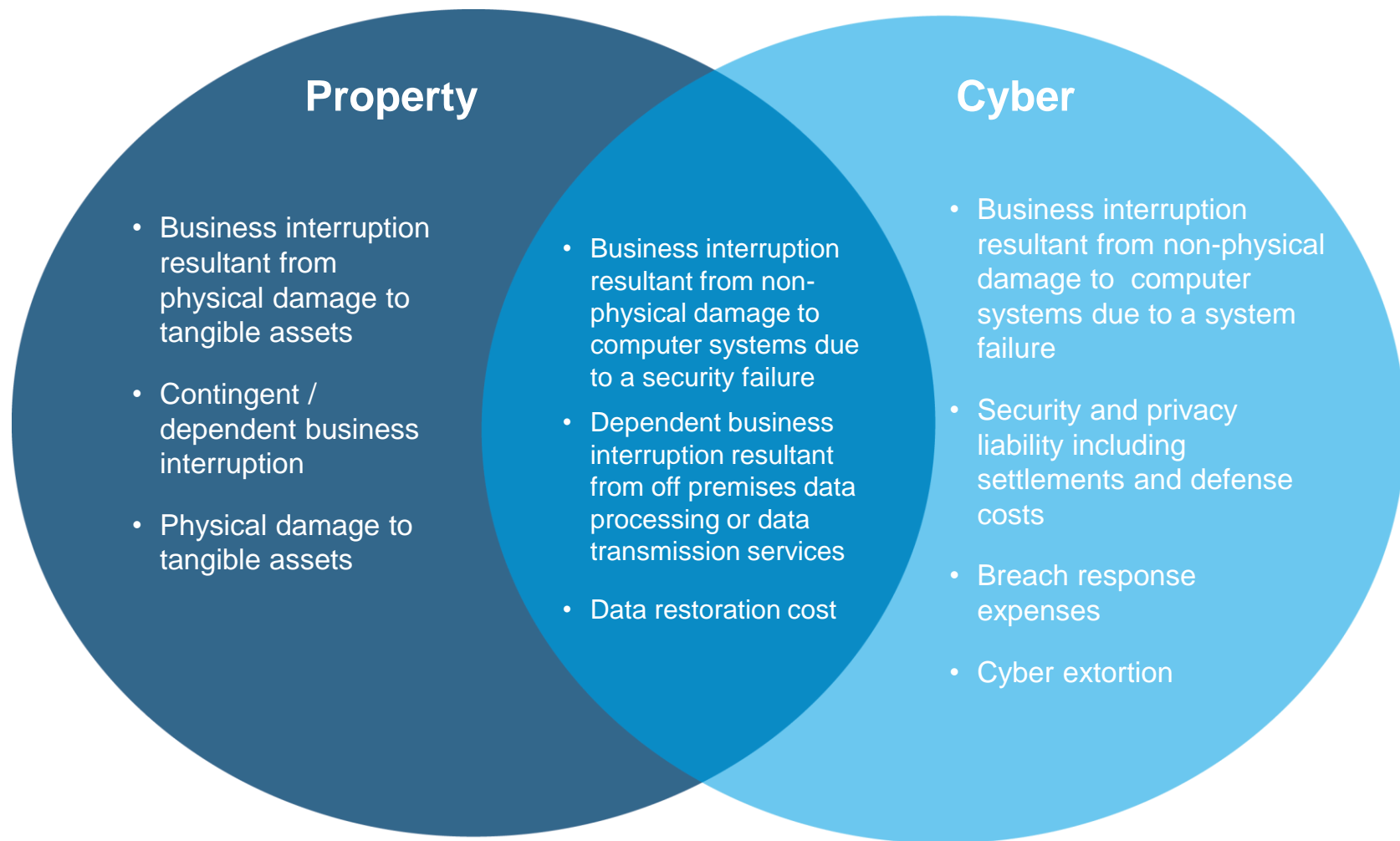
- Trustwave data taken from the 2015 Trustwave Global Security Report (n = 574)
- Mandiant data taken from the 2015 Mandiant MTrends Beyond the Breach study
- Ponemon data taken from the Ponemon Institute 2015 Cost of Data Breach Study: Global Analysis (n = 350)

Cyber – First Party Coverage Trigger: Discovery versus Retroactive Date



This slide is meant for educational purposes. Please see the applicable policy language to understand how coverage is triggered for your Cyber policy.

Cyber Coverage versus Property Form*





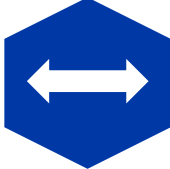


*Coverage in both forms can vary materially from carrier to carrier and base forms to manuscript policy forms

Coverage Considerations for Property and Cyber

Coverage Element	Property	Cyber
Trigger of Coverage	Trigger is physical loss or damage to data	Trigger is the cause of loss or damage (i.e. breach of network security arising out of an unauthorized access or virus transmission)
Waiting Period	24 or 48 hour waiting period, but if met, indemnity under the policy starts at the time of the physical loss, subject to policy deductible	6 to 12 hour waiting period retention, and indemnity under the policy starts after the waiting period is exhausted
Physical Damage of Computer Systems	Covered under Data, Programs, Software	Not covered
Non-Physical Damage of Computer Systems	Covered under Time Element	Covered according to cyber insuring agreements
Physical Damage to Other Tangible Assets	Need review endorsements	Not covered
Non-Physical Damage to Other Tangible Assets	N/A	Covered according to cyber insuring agreements

Cyber Liability Insurance Market Update

 <p>Capacity</p>	 <p>Coverage</p>	 <p>Claims & Losses</p>	 <p>Retentions</p>	 <p>Pricing</p>
<p>Capacity is continuing to grow across geographies</p>	<p>Coverage continues to evolve in favor of insureds</p>	<p>Stronger data gathered as more breaches reported</p>	<p>Retentions are <i>generally</i> trending upwards</p>	<p>Pricing has started to stabilize</p>
<ul style="list-style-type: none"> ▪ Over 65 unique insurers providing cyber liability capacity ▪ Capacity is available domestically (primary and excess), the UK (primary and excess) and Bermuda (excess only) ▪ Of the primary market place, there continues to be a growing number of insurers developing appetites for large, complex risks ▪ There is over \$500M in theoretical capacity available in the cyber marketplace 	<ul style="list-style-type: none"> ▪ Coverage breadth and limit availability is expanding ▪ Insurers continue to differentiate their offerings with new or enhanced coverage components ▪ Breach response coverage continues to increase and expand to meet insured's needs 	<ul style="list-style-type: none"> ▪ Complexity of breaches drives increase in incident response expenses incurred by insureds ▪ Increasingly punitive legal and regulatory environment ▪ Plaintiff's bar continues to advance proof of "damages" theories in security / privacy context ▪ Open privacy-related litigation can take years to conclude ▪ Policies are responding, allowing better tracking of claims payments 	<ul style="list-style-type: none"> ▪ Retentions of all levels are available in the market, but can vary greatly based on industry class, size and unique exposures ▪ Recent market pressure has led to increased retentions, sometimes significantly ▪ Adjusting retentions <i>can</i> lead to increased coverage and / or limit pricing flexibility 	<ul style="list-style-type: none"> ▪ Due to the competition in the marketplace, pricing is more competitive ▪ Some insureds have secured significant coverage improvements as a result of paying slightly higher premiums

Note: This is a general summary and could vary based on client industry and size

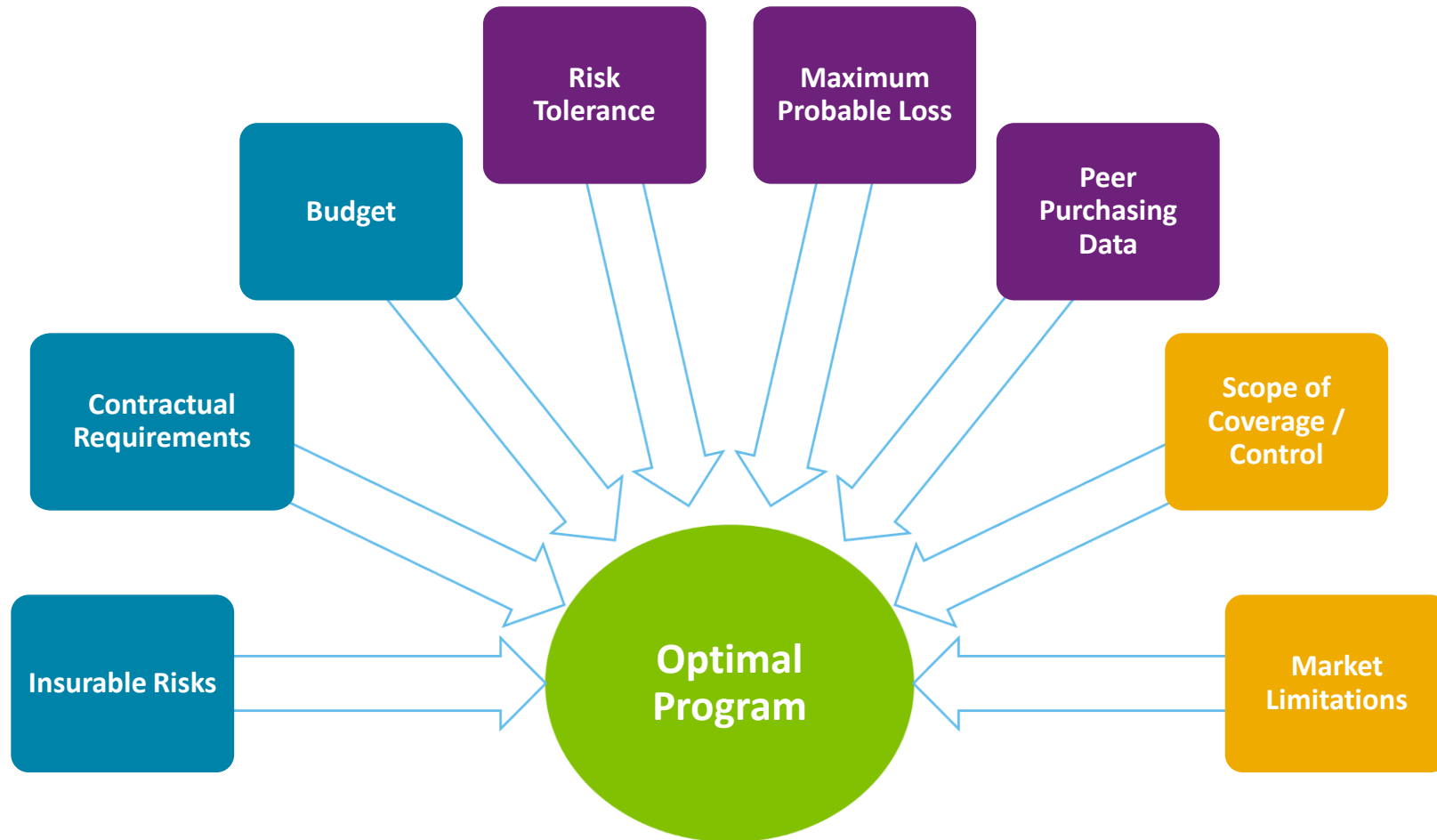
Cyber Liability Benchmarking – Financial Institutions

Unlike other lines of coverage where metrics are more easily transferable (directors and officers or property, where market cap or total insurable values provide a rating base), cyber liability, including security, privacy, and media liability coverage are specialized and broad data sets that cannot be easily compiled. Decisions to buy a certain cyber liability limit or retention could be based on contractual requirements, on prioritizing a specialized component of coverage, or on a certain company's perception of risk. Because the various coverage modules are offered on an “a la carte” basis, included coverage and premium may vary significantly even for companies of similar revenue size and business operations.

Revenues: \$0 - \$250M
Sample Size: 166

Coverage	Primary Limit	Total Limits	Retention	Primary Price Per Million
1 st Quartile	\$1,000,000	\$1,000,000	\$25,000	\$6,450
Median	\$3,000,000	\$3,000,000	\$50,000	\$9,334
3 rd Quartile	\$5,000,000	\$5,000,000	\$75,000	\$13,205
Average	\$3,576,471	\$6,047,059	\$78,147	\$10,197
Maximum	\$10,000,000	\$160,000,000	\$1,000,000	\$35,900

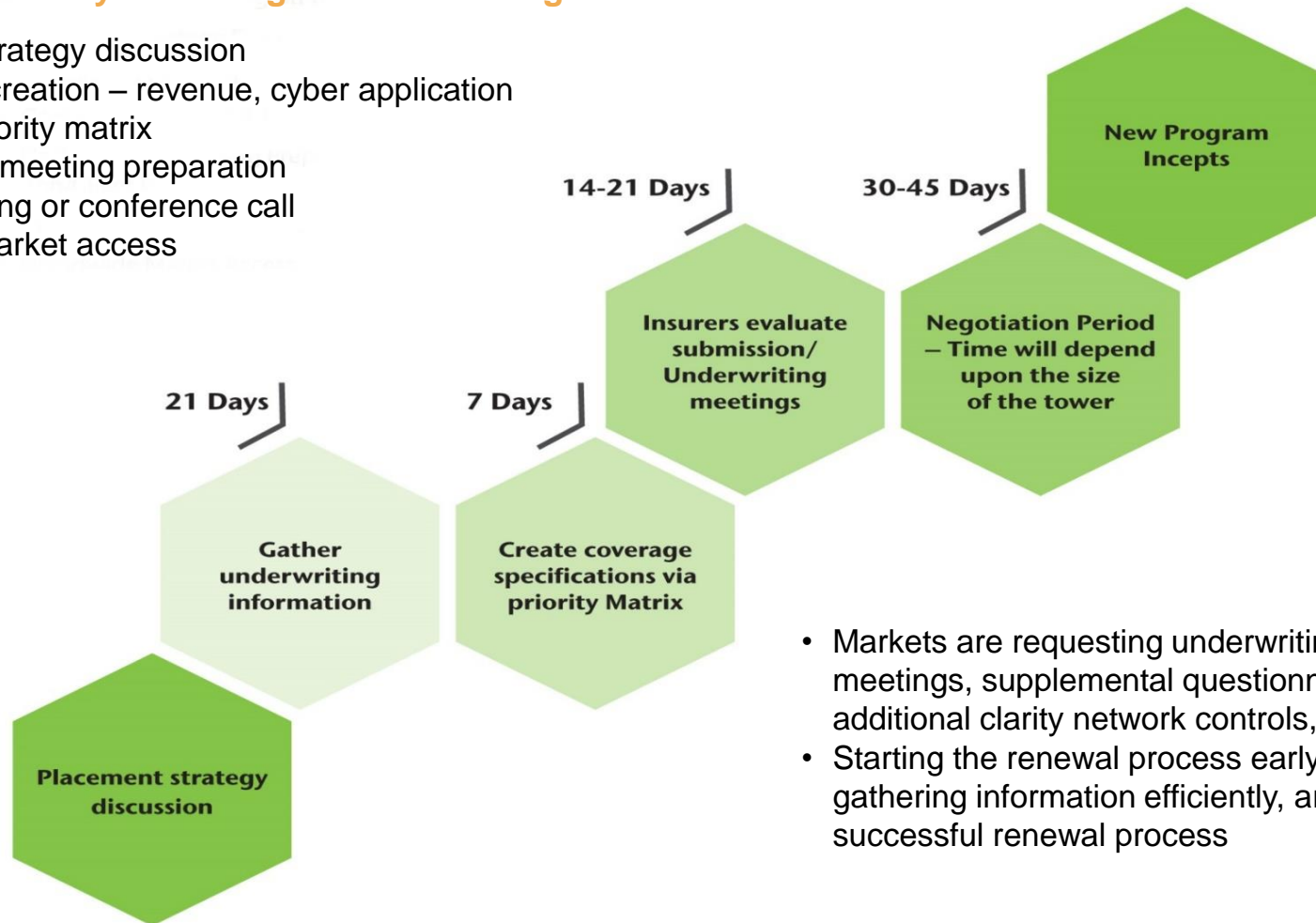
Optimal Cyber Program



Differentiating Our Clients

The key to a successful go to market strategy is to differentiate our clients. We do this by executing on the following:

- Placement strategy discussion
- Submission creation – revenue, cyber application
- Coverage priority matrix
- Underwriting meeting preparation
- Market meeting or conference call
- Worldwide market access



- Markets are requesting underwriting meetings, supplemental questionnaires, additional clarity network controls, etc.
- Starting the renewal process early, and gathering information efficiently, are key to a successful renewal process

Aon Cyber Solutions Framework

