

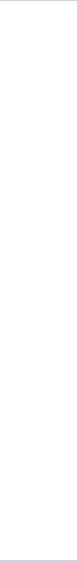
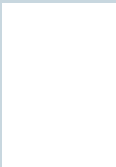
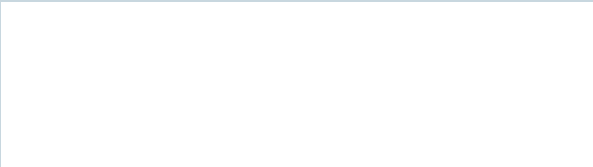
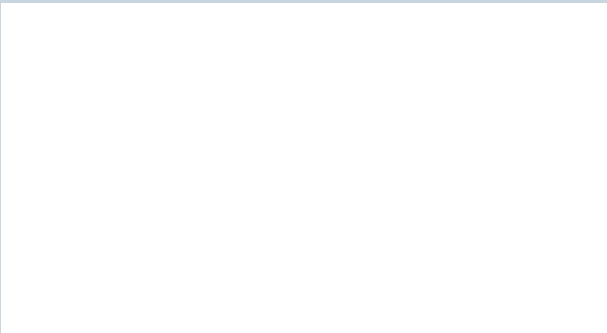
NCOIL: Cyber Risk & Insurance Presentation

Jim Wrynn
Senior Managing Director
Global Insurance Services
FTI Consulting

Tim Golden
Assistant Vice President
Cyber
Chubb Insurance

Jeffrey Schermerhorn
West Region Practice Leader
Cyber
Willis Towers Watson

Threat Landscape



The Cyber-Threat Landscape

Highly Capable Nation-State Actors

Targets

Government institutions, defense contractors, financial institutions, insurance companies, media organizations, healthcare industry, aerospace industry, critical infrastructure, etc.

Motivations

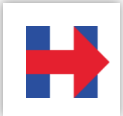
Espionage, Propaganda Disruption/ Destruction, Financial Gain



Sony
Pictures



Democratic
Party



Clinton
Kaine



United States
Office of Personnel
Management



Ukraine



Bangladesh
National Bank



The Cyber-Threat Landscape

Advanced Cyber Threats



Insider Threat

*Disgruntled employee, double agents
— knows your organization well.*



Hacktivist

*Causes disruption and reputational
and operational damage.*



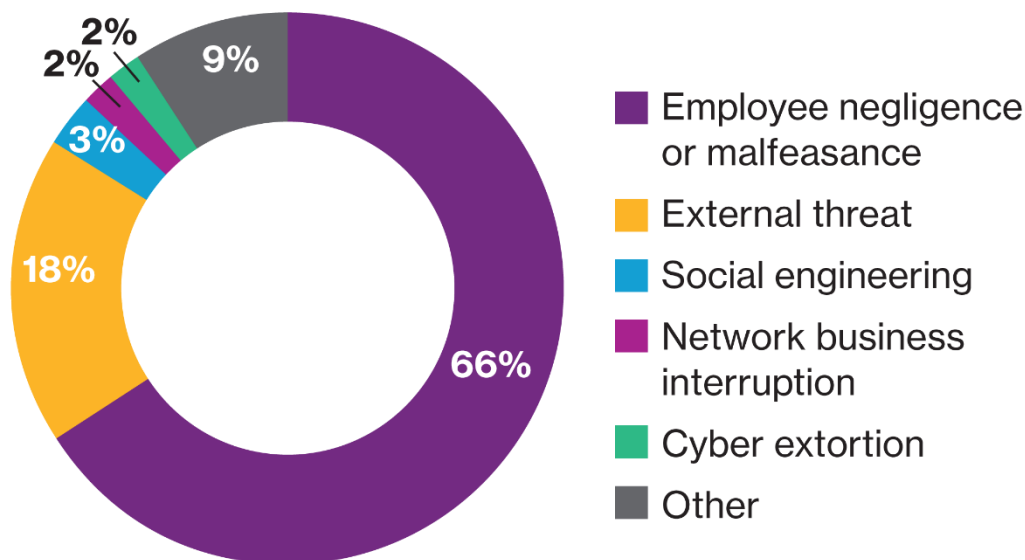
Organized Criminal Groups

*Sophisticated cyber-gangs
specializing in financial crimes.*

WTW claims data: Employee actors are top source of breaches

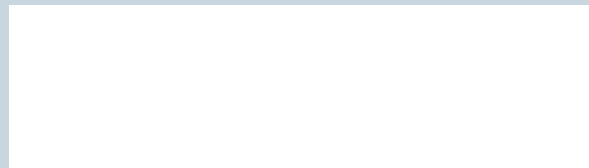
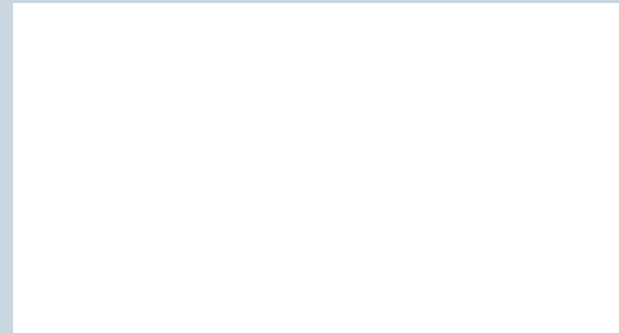
- Employee negligence or malicious behaviors are the most common source of cyber incidents
- The workplace is thus a major influence in mitigating cyber risk— using all the tools at an organization's disposal, such as:
 - Strong culture
 - Effective recruitment, onboarding and induction
 - Targeted training, compliance and incentive policies

Percentage of claims by breach








Source: Willis Towers Watson claim data

Cyber Insurance Market Discussion



State of the Cyber Insurance

 Capacity	 Coverage	 Claims & Losses	 Premiums & Retentions	 Markets
Plentiful	Expanding	Rising	Normalizing	Unaligned
<ul style="list-style-type: none"> With over 60 markets offering some form of cyber coverage, there is over \$600M of capacity available in the marketplace Over the coming year, we expect additional carriers to develop primary forms and compete for business Many carriers have released updates to their existing primary forms and other others are in the process of developing new revisions to their forms Primary and Excess capacity are available domestically and in London markets. Excess capacity over \$50M is available in Bermuda New capital and capacity will continue to flow into the excess marketplace, providing insurance buyers with more options 	<ul style="list-style-type: none"> Cyber product offerings vary widely, there are no uniform set of coverage terms, exclusions, definitions, or conditions The need to manuscript insuring agreements to specific industries and client exposures is necessary The scope of coverage continues to expand to include traditional Property coverages such as Business Interruption and Systems Failures but there is great variation, with regard to waiting periods and coverage triggers Coverage for Bodily injury and Property Damage is now being contemplated with the expansion of the Internet of Things (IoT) in healthcare, critical infrastructure, utilities, energy and manufacturing industries Traditional Crime Coverage for Social Engineering and Theft of Money is expanding 	<ul style="list-style-type: none"> Ransomware/Extortion claims dominated 2016, FBI reported a 300% increase in attacks since 2015 Over 66% of claims emanate from Human Behavior Insurers' are starting to see at least 2-3 business interruption claims a year with losses exceeding the waiting period Underwriting concerns over business interruption and property damage losses stemming from cyber incidents will continue to heighten as claims develop The costs associated with managing cyber and privacy claims including forensic investigations and defending regulatory actions and associated fines are on the rise 	<ul style="list-style-type: none"> Retentions at all levels are available but can vary greatly based on industry class, size of organization and particular exposures Insurers' have tightened pricing and retention guidelines for companies that have not addressed vulnerabilities Depending on loss history and claims experience, pricing is beginning to stabilize First time-buyers are enjoying competitive market conditions Renewal pricing range from flat to 15% increases depending on the security controls and privacy protections in place 	<ul style="list-style-type: none"> The marketplace remains unaligned on pricing, retentions and sub-limits Markets continue to insert InfoSec professionals into the underwriting process and are getting more granular with submission questions Standard applications are becoming obsolete for large organizations with mature risk management programs. Insurers' continue to innovate and build out their pre-breach and post-beach response services There is considerable uncertainty surrounding expanding global regulation such as GDPR as well as the NYS DFS regulation and the potential for increased regulatory action claims and associated non-compliance fines/penalties Underwriters are exploring alternative channels like big data analytics to seek insured's security score to underwrite SMB's where specialization is limited

Cyber Liability

Coverage Overview

Liability coverage

Privacy liability	Defense and liability associated with your inability to protect personally identifiable information or corporate confidential information of third parties. The information can be in any format and breached intentionally or negligently by any person, including third party service providers to which you have outsourced information. Third party service providers include, but are not limited to, IT service providers.
Network security liability	Defense and liability costs associated with your inability to prevent your computer network from attacking the network of others.
Media liability	Tort liability associated with content you create, distribute or is created and distributed on your behalf , including social media content.

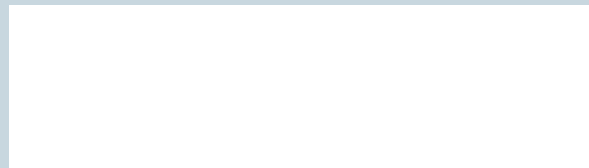
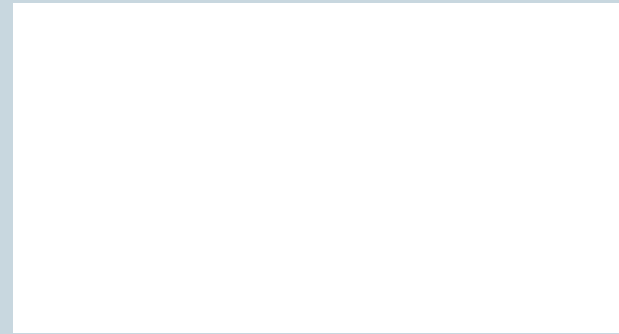
Direct (Loss mitigation coverage)

Breach response costs	Direct costs expended to mitigate a privacy breach. Costs typically include public relations expenses, notification, identity theft restoration, credit monitoring services and forensic/remediation expenses.
------------------------------	--

Direct (First party coverage)

Income loss/extra expense	Income loss/extra expense associated with your inability to prevent a disruption to your computer network caused by a computer attack or programming or software failure either: <ol style="list-style-type: none">1. on your network, or2. at your IT service provider hosting your application.
Data reconstruction	Your costs to recreate, recollect data lost, stolen or corrupted due to your inability to prevent a computer attack against your computer network.
Extortion costs	Your costs expended to comply with a cyber extortion demand.
Regulatory fines	Fines assessed by a regulatory body due to your data breach.

Events and Claims Scenarios





The Equifax Breach

How it Happened?

Hackers gained access to Equifax web servers in May of 2017

Web servers were compromised via Apache Struts vulnerabilities

Apache Struts is an enterprise web application framework

Once inside, hackers “moved laterally” by compromising internal systems and stole sensitive data



The Equifax Breach

Apache Struts Jakarta Multipart Parser Vulnerability (CVE-2017-5638)

CVE-2017-5638 was reported on March 08, 2017

Oracle released several Critical Patch Updates to address the flaw

Oracle warned users of the critical vulnerability and urged them to upgrade to the newly released patched version immediately

Leaving systems unpatched enabled hackers the ability to remotely execute malicious code and gain unauthorized access



Proper Cybersecurity Policy, Controls, and Governance

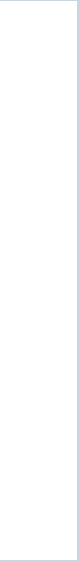
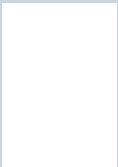
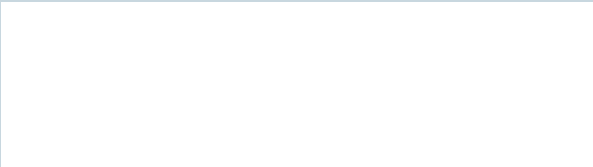
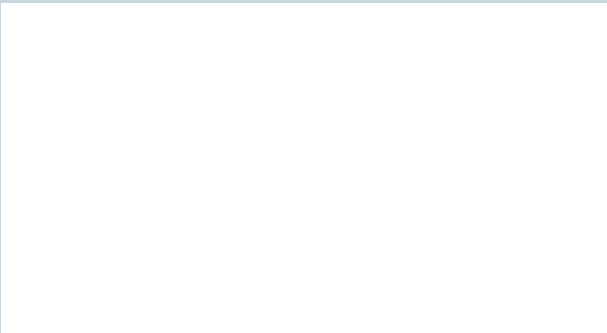
The Equifax breach was easily avoidable; critical patches should always be installed ASAP

Preventative steps: Regular vulnerability assessments; proper oversight and enforcement of patching policies

Cybersecurity policy, controls, and governance is essential in protecting organizations from emerging threats

Organizations require a CISO empowered to enforce industry standard best practices and strict cybersecurity controls

Regulatory Changes





Cybersecurity Impacts on Regulatory Requirements

Regulators are adapting and becoming more aware of the increase in cybersecurity risk from sophisticated attacks

For example NY DFS is requiring companies to have a well defined cybersecurity programs led by a CISO

Other regulators will continue to come in line and adapt similar regulatory requirements

Challenges differ for organizations with well established security budgets and smaller ones without dedicated cybersecurity staff



Cybersecurity Impacts on Regulatory Requirements

Solutions to aid in compliance

Virtual CISO Services – Outsource the CISO position to firms that provide CISO responsibilities as a service

Virtual SOC – Outsource security operations, threat monitoring, and detection services to dedicated security firms

Regularly employ third party firms to conduct penetration tests of your organization to reveal critical vulnerabilities

Work with advisory firms to assess current regulatory compliance and strategically enact organizational and policy changes
