


Cyber-Security & Cyber-Risk Insurance Fundamentals




Introduction to Cyber Insurance

By: Uzair Mirza


16th July 2019

16th July 2019 PII Workshop 1

Cyber-Security & Cyber-Risk Insurance Fundamentals




Background



16th July 2019 PII Workshop 2

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Cyber Environment

- Growing digital data and its connectivity with outside world
 - Mobile apps
 - Automated systems
 - Social media
 - Cloud computing
- Companies collecting, storing and processing large amount of data of all kinds

16th July 2019 PII Workshop 3

Cyber-Security &
Cyber-Risk Insurance Fundamentals



Cyber Environment

To exploit new business opportunities, by breaking down barriers and providing the capability to drive work beyond the boundary of just one team or one organization.

The pace of change in digital transformation is exponential. There are new ways to engage with customers, more innovation in the workforce and more opportunities to harness data insights as just a few of the benefits that digital transformation brings.

16th July 2019 PII Workshop 4

Cyber-Security &
Cyber-Risk Insurance Fundamentals



Cyber Environment

Virtually every organization is on the path to digital

- Retailers
- Banks/FIs
- Travel & Hospitality
- Healthcare
- Manufacturing
- Utility Companies
- Construction

Just name it

16th July 2019 PII Workshop 5

Cyber-Security &
Cyber-Risk Insurance Fundamentals



Cyber Environment

Increasing reliance on technology and connectivity leads to increasing Cyber exposure for all types of organizations

Cyber-crime, media liabilities, and a heavy reliance on the uptime of the network, for example.



16th July 2019 PII Workshop 6

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Cyber Environment

There are new business exposures faced by commercial organizations, primarily driven by continually evolving e-commerce laws.

Cyber liability to Third Parties, Network Security, Business Interruption and Loss of Data are just some of the new liabilities businesses need to build into their risk management and risk transfer strategies

16th July 2019 PII Workshop 7

Cyber-Security &
Cyber-Risk Insurance Fundamentals



Cyber Risk Defined

Exposures emanating from computer networks and the internet

Any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability, or integrity of data or services. The impairment of operational technology (OT) eventually leads to business disruption, (critical) infrastructure breakdown, and physical damage to humans and property.

16th July 2019 PII Workshop 8

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Challenges

- Hackers/Fraudsters are just next door
- No State Boundary
- Local Incident –Global Effect
- State Sponsored Cyber Attacks


16th July 2019 PII Workshop 10

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Definition of Cybercrime

- Criminal activity committed using a computer especially to illegally access, transmit, or manipulate data
(Merriam Webster)
- Crime that takes place through the use of computers, computer technology or the Internet
(Black's Law Dictionary 2nd Ed)



16th July 2019 PII Workshop 11

Cyber-Security &
Cyber-Risk Insurance Fundamentals




How's of Cybercrime

- Users are a weak link in the security infrastructure
 - Phishing and spearphishing
 - Identity theft
 - CEO Fraud/Business Email Compromise (BEC)/Whaling
- Ransomware
- Data breaches and loss of customer data
- Malware and viruses
- Social media

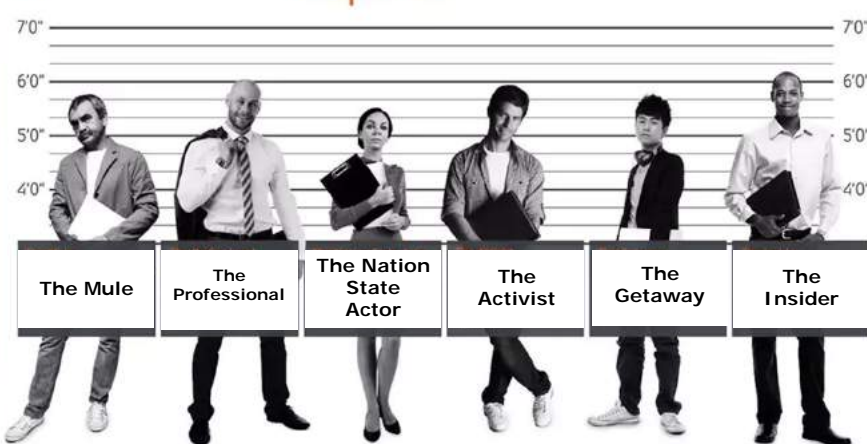
This list is not exhaustive

16th July 2019 PII Workshop 12

Cyber-Security &
Cyber-Risk Insurance Fundamentals



The Unusual Suspects




The Mule	The Professional	The Nation State Actor	The Activist	The Getaway	The Insider
----------	------------------	------------------------	--------------	-------------	-------------

The six types of cybercriminals identified by BAE

16th July 2019 PII Workshop 13

Cyber-Security &
Cyber-Risk Insurance Fundamentals




What is Cyber Liability?

The simplest definition for cyber liability is legal responsibility for "cyber" assets, which might include email, websites, customer information, and any other data or material stored digitally (on the cloud, on a machine's hard drive, or on external storage devices).

Liability arising out of the loss of or unauthorized access to private and/or confidential information in your care, custody & control

16th July 2019 PII Workshop 14


Cyber-Security &
Cyber-Risk Insurance Fundamentals



What is Private Information?

- **Personally Identifiable Information (Non-Public)**
 - CNIC Number
 - Drivers License Number
 - Debit/Credit Card Numbers
 - Bank Account Numbers
 - Passport Number
- **Confidential Information (Business)**
 - Trade Secret
 - Information subject to a confidentiality agreement
- **Protected Healthcare Information**
- **First and Third Party Information**

16th July 2019 PII Workshop 15

Cyber-Security & Cyber-Risk Insurance Fundamentals 


What is a Data Breach?

Release or disclosure of PII/Confidential information to an unauthorized individual/entity that:

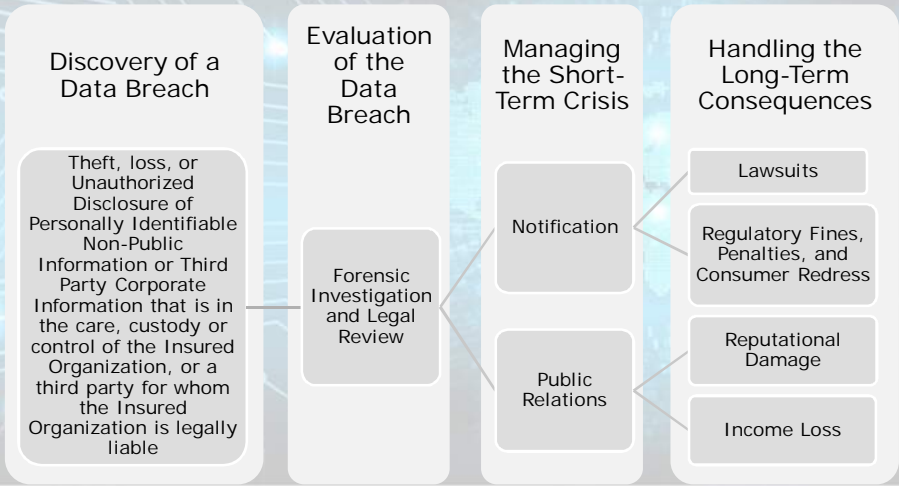
- May cause the person inconvenience or harm (financial / reputational)
 - Names, home addresses, email addresses, usernames, passwords, family-member information, etc.
- May cause inconvenience or harm to your customers, employees or business partners (financial / reputational)
 - Information that relates to customers
 - Information that relates to current / former employees and applicants
 - Information relating to internal matters (business plans, employment disputes, Union negotiations)

16th July 2019
PII Workshop

16

Cyber-Security & Cyber-Risk Insurance Fundamentals 

A Simplified View of a Data Breach



```

    graph LR
      A["Discovery of a Data Breach  
Theft, loss, or Unauthorized Disclosure of Personally Identifiable Non-Public Information or Third Party Corporate Information that is in the care, custody or control of the Insured Organization, or a third party for whom the Insured Organization is legally liable"] --> B["Evaluation of the Data Breach  
Forensic Investigation and Legal Review"]
      B --> C["Managing the Short-Term Crisis  
Notification  
Public Relations"]
      C --> D["Handling the Long-Term Consequences  
Lawsuits  
Regulatory Fines, Penalties, and Consumer Redress  
Reputational Damage  
Income Loss"]
    
```

16th July 2019
PII Workshop

17

Cyber-Security &
Cyber-Risk Insurance Fundamentals

PII
Precision Insurance Institute
Since 1911

Crime And Cyber Coverage

```

graph LR
    ATTACK[ATTACK] --> FUNDS[FUNDS TRANSFER]
    EMPLOYEE[EMPLOYEE ACTION] --> DATA[DATA TRANSFER]
    FUNDS --> CRIME[CRIME]
    DATA --> CYBER[CYBER]
    CRIME --> DIRECT[DIRECT LOSS]
    CYBER --> ECONOMIC[ECONOMIC DAMAGES]
  
```

16th July 2019 PII Workshop 18

Cyber-Security &
Cyber-Risk Insurance Fundamentals

PII
Precision Insurance Institute
Since 1911

The Evolution of Cyber Coverage

- The roots of cyber coverage go back about 20 years. Back then, technology companies bought errors and omissions (E&O) insurance, which over time, was extended to include things like a software product bringing down another company's network, unauthorized access to a client system, destruction of data, or a virus impacting a customer.

16th July 2019 PII Workshop 19

The Evolution of Cyber Coverage


- The companies that bought this early cyber insurance were generally in the technology space and already buying E&O insurance. The technology coverage, often called “network security” or “Internet liability” was an add-on.
- Five to 10 years ago, we saw these “network security” policies expand into the privacy space by providing clear coverage for breaches of confidential information.

Cyber Insurance Today

A cyber policy is designed to cover privacy, data and network exposures and provide peace of mind.

The policy is developing as risks and new exposures emerging

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Cyber Insurance Today

- Each insurer's policy is different.
- Coverages vary depending upon business' requirement and insurers' capacities
- Policy wordings comparison is complex.
- However there are certain common coverage elements.

16th July 2019 PII Workshop 22

Cyber-Security &
Cyber-Risk Insurance Fundamentals



Cyber Insurance Today

- Cyber insurance generally covers financial losses that result from data breaches and other cyber events.
- Many policies include both first-party and third-party coverages.
- The most common coverages are;

16th July 2019 PII Workshop 23

Cyber-Security &
Cyber-Risk Insurance Fundamentals




First Party Coverages

- First-party coverages apply to losses sustained by the insured directly. An example is a damage to company's electronic data files caused by a hacker.
- First-party coverages are often subject to a deductible.

16th July 2019 PII Workshop 24

Cyber-Security &
Cyber-Risk Insurance Fundamentals




First Party Coverages

- Many policies cover **Loss or Damage to Electronic Data**, theft, disruption or corruption of electronic data. They also cover damage or theft of data stored on computer system that belongs to someone else. For a loss to be covered, it must result from a covered peril such as a hacker attack, a virus, or a denial of service attack.
- The policy generally covers the costs to restore or recover lost data. It may also cover the cost of outside experts or consultants hired to preserve or reconstruct data.

16th July 2019 PII Workshop 25

Cyber-Security &
Cyber-Risk Insurance Fundamentals




First Party Coverages

- Many policies cover **Loss of Income or Extra Expenses** incurred to avoid or minimize a shutdown of business after computer system fails due a covered peril.
- Cyber policies cover income losses and extra expenses that result from an interruption of computer system by a covered peril. Property policies cover income losses and extra expenses that result from an interruption in business operations caused by physical damage to covered property, which does not include electronic data.

16th July 2019 PII Workshop 26

Cyber-Security &
Cyber-Risk Insurance Fundamentals




First Party Coverages

- **Cyber Extortion** coverage applies when a hacker or a cyber thief breaks into the computer system and threatens to commit a nefarious act, for instance, to:
 - damage data, introduce a virus, or shut down computer system
 - subject the computer system to a denial of service attack or threaten to release confidential data unless the victim pays the sum demanded.
- Extortion coverage typically applies to expenses incurred (with the insurer's consent) to respond to an extortion demand, as well as the money paid to the extortionist.

16th July 2019 PII Workshop 27

Cyber-Security &
Cyber-Risk Insurance Fundamentals



First Party Coverages

- Policies may cover **Notification Costs** incurred in informing parties affected by the data breach by government statutes or regulations. They may also include the cost of hiring an attorney to assess the firm's obligations under applicable laws and regulations. Some policies cover the cost of providing credit monitoring services for those affected by the breach. Some also cover the cost of setting up and operating a call center.

16th July 2019 PII Workshop 28

Cyber-Security &
Cyber-Risk Insurance Fundamentals




First Party Coverages

- Some policies cover the costs incurred for marketing and public relations to protect company's reputation following a data breach. This coverage may be referred to as **Crisis Management**

16th July 2019 PII Workshop 29

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Third Party Coverages

- Most cyber policies include more than one type of liability coverage. These coverages apply to damages or settlements that result from covered claims. They also cover the cost of defending against such claims.
- Defense costs may reduce the limit of insurance. Virtually all cyber liability policies are claims-made. Some third-party coverages may be subject to retention.

16th July 2019 PII Workshop 30

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Third Party Coverages

- **Network Security Liability** - Policies may cover lawsuits alleging that the insured failed to adequately protect data belonging to customers, clients, employees or other parties resulting in a data breach or inability of others to access data on company's computer system. Coverage may apply if the data breach or inability to access system is due to a denial of service attack, a virus, malware or unauthorized access and use of computer system by a hacker or rogue employee.

16th July 2019 PII Workshop 31

Cyber-Security &
Cyber-Risk Insurance Fundamentals



Third Party Coverages

- **Network Privacy Liability** - Network privacy liability insurance covers lawsuits based on allegations that the company failed to properly protect sensitive data stored on its computer system. The data may belong to customers, clients and other parties. Some policies cover liability arising from the release of private data (such as social security numbers) belonging to employees.

16th July 2019 PII Workshop 32

Cyber-Security &
Cyber-Risk Insurance Fundamentals



Third Party Coverages

- **Regulatory Response** - Cyber insurance covers the legal, technical or forensic services necessary to assist the policyholder in responding government inquiries relating to a cyber attack, and provides coverage for fines, penalties, investigations or other regulatory actions

16th July 2019 PII Workshop 33


Third Party Coverages

- **Electronic Media Liability** - Patents, software, and copyright are covered by intellectual property insurance policy, and not by a cyber policy. In some cases, however, a cyber policy can cover the defense cost for copyright infringement claims. But such claims should be a consequence of actions resulting from publication of electronic data on the Internet directly from a covered peril.

Other Coverages

- Other coverages that may be available under a cyber liability policy include various crime coverages such as computer fraud, funds transfer fraud, and cyber terrorism (acts of violence committed for political purposes). Some insurers have developed cyber liability policies tailored to specific industries. For example, one policy may be designed for businesses in the healthcare industry while another policy is intended for financial institutions.

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Sublimits, Deductibles and Limits in Cyber Coverage

- All of the first-party coverage elements, and the fines and penalties aspect of the third-party coverage, are typically offered as a sublimit of liability.
- In addition to a dollar deductible (which ranges widely depending on the size of the policy and the company being insured), most policies include a time element deductible to trigger the business interruption coverage.

16th July 2019 PII Workshop 36

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Common Exclusions

- **Retroactive Date:** No cover for events/circumstances/ viruses that happened before the retroactive date
- **Inception Date:** No cover for claim or any acts, facts, or circumstances occurred or known before the inception date

16th July 2019 PII Workshop 37

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Common Exclusions

- **Bodily Injury:** When a vital business data is breached, it does not mean that the person is directly physically injured because of it and hence the claim is excluded. Also no cover for emotional distress and anguish caused by such events.

16th July 2019 PII Workshop 38

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Common Exclusions

- **Property Damage:** No cover for hardware, however restoration expenses for data and computer programs covered
- **Loss of electronic device:** When an employee loses a company-issued portable electronic device, the coverage for the same is excluded from the insurance.

16th July 2019 PII Workshop 39

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Cyber Insurance Underwriting

General business information allows the insurer to understand the extent of the organization's exposure to cyber threats and to better assess what solution to offer;

- Main activities: sector, type of products and services
 - Percentage of activity in B-to-C business
 - Percentage of activity in B-to-B business
 - Geographical area (countries, jurisdictions)
 - Turnover, income

16th July 2019 PII Workshop 40

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Cyber Insurance Underwriting

- IT Security & Monitoring Policy
- Amount of data & PII
- HR
- Suppliers & Vendors
- Internal Audit

16th July 2019 PII Workshop 41

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Cyber Scenario

Hackers breach systems of a large retailer using a spear-phishing attack on employee emails and gain access to the log-in credentials and commercially sensitive and clients' personal information. Records are sold on the dark web and details of the breach become public. Impacted commercial clients commence proceedings against the retailer.

16th July 2019 PII Workshop 42

Cyber-Security &
Cyber-Risk Insurance Fundamentals



Cyber Scenario

Immediately upon discovering the breach, the retailer will require forensic investigation specialist to investigate and determine;

- how the breach occurred,
- what information was released and
- how to stop the breach, if it is continuing.

The retailer may also require crisis management/ public relations team to help develop and execute a media strategy for managing the public narrative relating to the breach.

16th July 2019 PII Workshop 43

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Cyber Scenario

- The retailer will also require specialized assistance and legal guidance for handling all the aspects of the breach separate from dealing with any claims against the retailer.
- The retailer may have to notify individuals who could be affected by the breach.

16th July 2019 PII Workshop 44

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Cyber Scenario

The retailer will require legal representation in case legal proceedings are brought by its clients and could have to pay damages at the conclusion of the proceedings.

In addition the retailer could face a regulatory investigation or proceedings for unauthorized release of consumer data, and ultimately may have to pay fines/penalties

16th July 2019 PII Workshop 45

Cyber-Security &
Cyber-Risk Insurance Fundamentals




Cyber Scenario

A cyber insurance policy in this scenario could potentially cover;

- legal costs and damages from claims alleging privacy breach or network security failure.
- cost of forensic investigation,
- legal services,
- call center services,
- crisis management and
- public relations services

16th July 2019 PII Workshop 46

Cyber-Security &
Cyber-Risk Insurance Fundamentals



Cyber Scenario

With respect to indemnity under different cyber insurance policies, following could impact potential coverage:

1. Policy may require the insured to receive express, written permission from the insurer before incurring any costs in relation to managing/ mitigating a breach.
2. Policy may be subject to a retroactive date.

16th July 2019 PII Workshop 47

Blurred Lines

Medidata Solutions vs. Federal Insurance, 2017 NY


The claim arose after employees in Medidata’s finance department were deceived into transferring that amount to a Chinese bank, based on emails that falsely appeared to come from the company’s president.

The claim was denied by the insurer on a number of bases, including that there had been no manipulation of Medidata’s computers and Medidata “voluntarily” transferred the funds. However the court said the manipulation of code in the email messages amounted to the kind of “deceitful and dishonest access” required to trigger cover under the policy. A sufficient causal connection was established between the fraudulent conduct and the resulting transfer to trigger a claim under that policy.

Blurred Lines

The case demonstrates the overlap that exists when the wording in a fraud policy is wide enough to cover cyber-triggered events, or where cyber policies cover “social engineering” with a fraud element.


In the Medidata case, Federal Insurance Company had to pay out a social engineering claim (USD4.8Mn) under the fraud provision. The insurer did not anticipate the cyberattack vector—in this case, social engineering through email—under its fraud provision, either in drafting the wording of the coverage or underwriting and rating the premium.

Cyber-Security & Cyber-Risk Insurance Fundamentals 

Do you believe funds transfer fraud loss due to social engineering is better covered by a cyber policy or a crime policy?

- The issue of cyber versus crime policies for funds transfer fraud/social engineering has been a hotspot for discussion and legal activity in the past year. Although 66% of insurers offer this cover frequently or on occasion in cyber policies, just over 70% of these respondents thought that it should in fact be covered under crime policies.

16th July 2019 PII Workshop 50

Cyber-Security & Cyber-Risk Insurance Fundamentals 

Do you believe funds transfer fraud loss due to social engineering is better covered by a cyber policy or a crime policy?

- On the other hand, brokers agree on both points. Just over half (53%) said that they feel a crime policy should respond, while 35% said cyber. Others see a blended response, with one broker saying, "Both: the crime should pick up the financial loss and the cyber should respond to deal with first-party costs for what clearly was a cyber intrusion."

16th July 2019 PII Workshop 51

Cyber-Security &
Cyber-Risk Insurance Fundamentals



Comprehensive Crime Policies

- Infidelity of employees
- Third party fraud
 - Documentary fraud
 - Electronic fraud
- Physical loss or damage
- Extortion
- Fees and expenses
- Social Engineering Extension

16th July 2019 PII Workshop 52


Cyber-Security &
Cyber-Risk Insurance Fundamentals



“There are only two types of companies: those that have been hacked and those that will be”

Robert Mueller
Director, FBI

16th July 2019 PII Workshop 53

Cyber-Security & Cyber-Risk Insurance Fundamentals 

Conclusions

Not “if” but “when”

- Information exists in multiple formats throughout an organization
- Information is subject to a multiple forms of loss

The costs of a data breach event may be significant!

- Notification Costs
- Credit Monitoring Expenses
- Defense Costs
- Cost of settlement or judgments

Costs generally not covered by traditional insurances

16th July 2019 PII Workshop 54

Cyber-Security & Cyber-Risk Insurance Fundamentals 

Conclusions

CRIME	RISK	CYBER
X	Data Breach Management Expense	✓
X	Legal Liability & Defense Cost	✓
X	Regulatory Investigation	✓
X	Loss of Income Due to Network Interruption	✓
X	Loss of Information Assets Due to Security Failure	✓
X	Cyber Extortion	✓
✓	Fraudulent Funds Transfers	✓
✓	Social Engineering (leading to loss of funds)	X
✓	Employee Theft	X
✓	Forgery	X

16th July 2019 PII Workshop 55