



# Cyber Risk & Insurance

## Global Risk & Pakistan Perspective

**Ram Garg CFA, MBA**  
Financial & Casualty Line  
J B Boda & Co (Singapore) Pte Ltd

**Karachi**  
**Insurance**  
**Institute**



## **Disclaimer:**

**The views, information and content expressed here in are those of the author and do not represent the views of any of J B Boda Group Companies. The information provided should not be provided as legal advice or a definitive statement of law in any jurisdiction. For such advice, an applicant, insured or reader should consult their own legal counsel.**

# AGENDA



- Market Landscape
- Marketplace - Demand & Supply
- Cyber Coverage
- Underwriting
- Cyber Risk Management & Assessment
- Claims & Incident Response Services
- Placement Consideration



---

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

**Robert Mueller**

Director, FBI

---

---


“We are in a day when a person can commit about 15,000 bank robberies sitting in their basement”

Robert Anderson

Executive Assistance Director, FBI's Criminal  
Cyber Response and Services Branch

---

## Cyber – An increasing Geopolitical Threat



*“most vexing security challenges are transnational security threats that transcend borders: climate change, piracy, infectious disease, transnational crime, cybertheft, and the modern-day slavery of human trafficking.”*

Susan Rice  
U.S. National Security Advisor



# Guess what we have in common ?



**DO ANYONE  
CLAIM THAT THEIR  
IT SECURITY  
PROTOCOLS MAKES  
THEM  
UNTOUCHABLE?**





**Hackers steal**

A row of five hoodlums wearing Guy Fawkes masks, dressed in black suits and ties, standing against a black background. The central figure is slightly larger and has their hands clasped in front of them.

**\$100 Million  
from Bangladesh**

# Hackers steal \$4.4m from Nepal bank in cyber-heist by abusing Swift network

■ Hackers abused Swift to steal approximately \$4.4 million.



*By Jason Murdock*

*November 7, 2017 18:31 GMT*



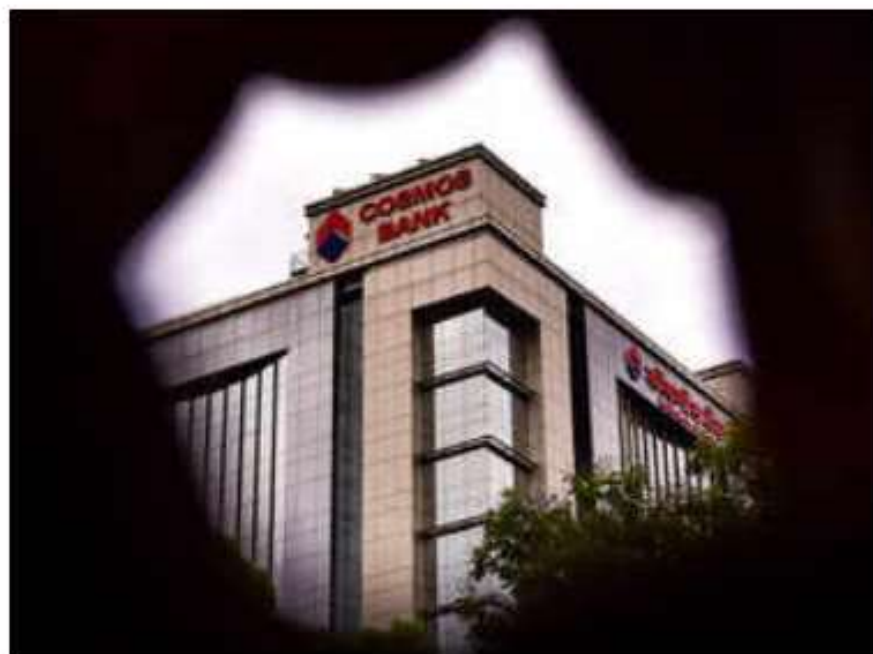
# Cosmos Bank's server hacked; Rs 94 crore siphoned off in 2 days

PTI | Updated: Aug 14, 2018, 09:31 PM IST



29  
Comments

Save



PUNE: Hackers managed to siphon off over Rs 94 crore through a malware attack on the server of Pune-based **Cosmos Bank** and cloning thousands of the bank's debit cards over a period of two days, a top official said.

The fraudulent transactions were carried out on August 11 and August 13 and the malware attack by the hackers originated in Canada, Cosmos Bank chairman Milind Kale told reporters here today.

*According to the FIR, the hackers used an unidentified*



Home **Mumbai** Entertainment Videos Photos Sports News Opinion Live

Mumbai Speaks Cover Story Crime Civic Other

HOME \ MUMBAI \ CRIME \ FRAUDSTERS DUPED STATE BANK OF MAURITIUS BY HACKING SWIFT SYSTEM: MUMBAI PO

## Fraudsters duped State Bank of Mauritius by hacking SWIFT system: Mumbai Police

Mumbai Mirror | Updated: Oct 13, 2018, 10:31 IST



A-

A+

By **Vallabh Ozarkar**

*State Bank of Mauritius claims to have frozen 90% of stolen money.*

The Mumbai Police's probe into the cyber attack on the city branch of the State Bank of Mauritius (SBM) has revealed that the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system – used for remittance



# Cyber Environment

- Growing digital data and its connectivity with outside world
  - Mobile apps
  - Automated systems
  - Social media
  - Cloud computing
- Companies are collecting, storing and processing large amount of data of all kinds
- Increasing reliance on technology and connectivity leads to increasing Cyber exposure for all kinds of organisations



# Source of Cyber Loss

State sponsored...



Criminals



Hacktivism..



For Fun..



Rogue employee...



Human error...



# Types of Cyber Attacks

Malware...



Code exploits..



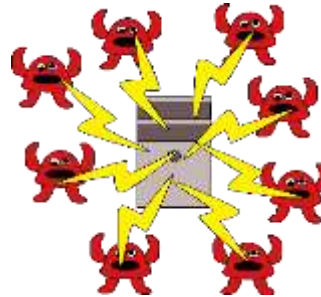
Ransomware..



Spear-phishing..



DOS attack...



Unauthorized access...





# MARKET LANDSCAPE



## Landscape

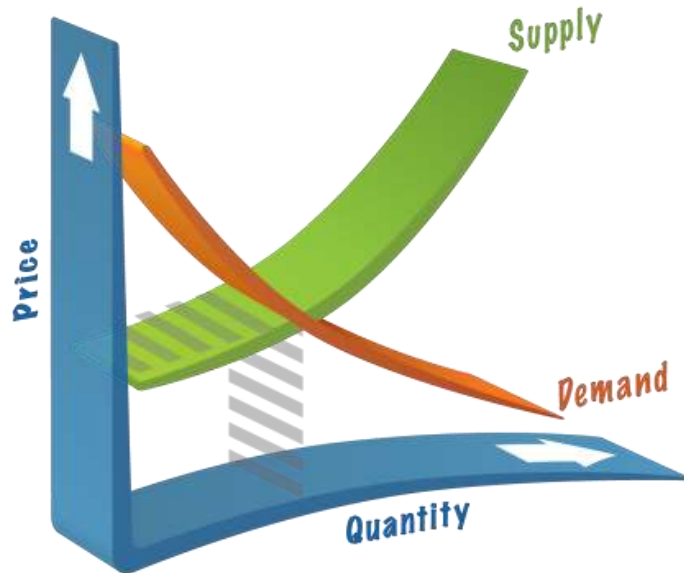
- Cyber insurance market is rapidly emerging and expected to ten-fold its size, reaching \$20 billion by 2025.
- However, the insurance industry is struggling with issues such as the lack of historical data, inadequate cybersecurity information, ever evolving cyberattacks, aggregation of cyber exposure, buyers' awareness, or the inexperience in underwriting, claims & responses management – final result is volatility and uncertainty surrounding this peril.

# Cyber Insurance/Reinsurance Market in Singapore/HK

## In its infancy

- 10+ insurers offer cover
- 2-3 Reinsurance capacity providers
- No standard policy wordings
- 15-50 underwriting questions
- High variation in premium
- Uncertainty of coverage
- Limited response service providers





# Cyber Insurance Marketplace

# Marketplace: Wide differences

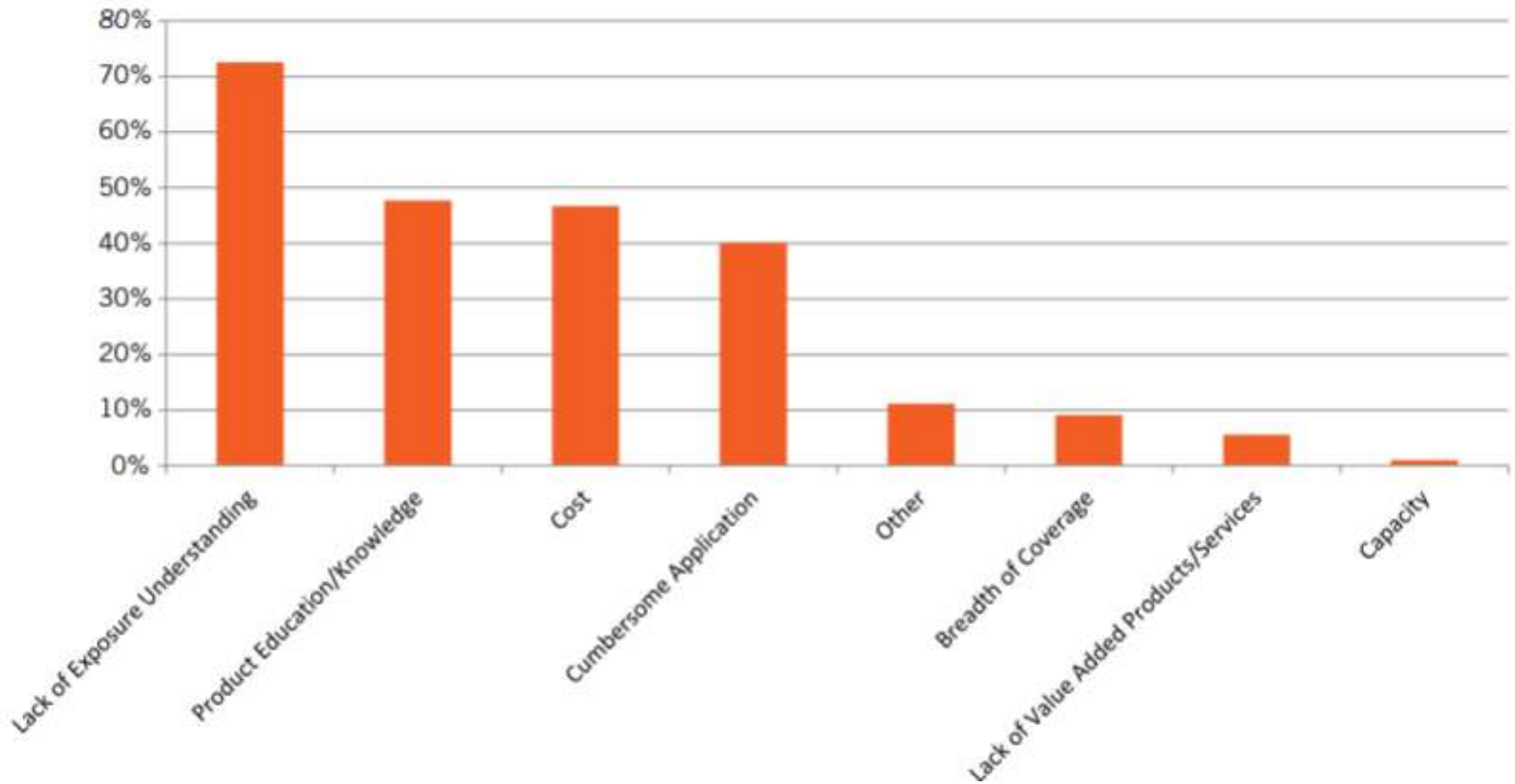
## Demand Side

- Poor awareness of the risk
- Inconsistent policy wordings
- Limited coverage
- Legal landscape remains in flux

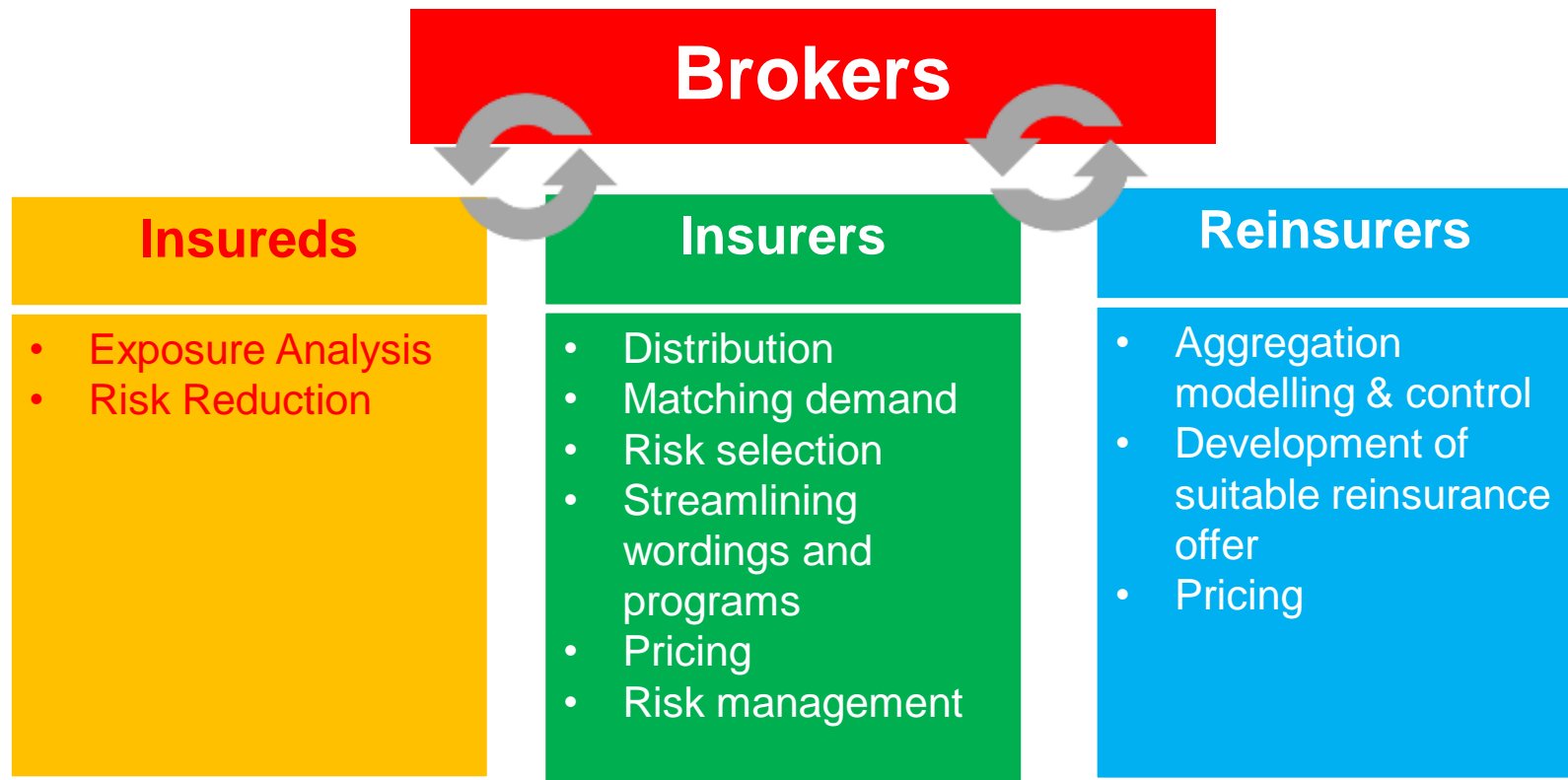
## Supply Side

- Rapidly evolving risk landscape
- Lack of understanding of exposures
- Accumulation risk uncertainty

# Obstacles to Selling Cyber Coverage According to Brokers



# Addressing Challenges in Risk Transfer





# Cyber Coverages

# Standalone Cyber Insurance Overview

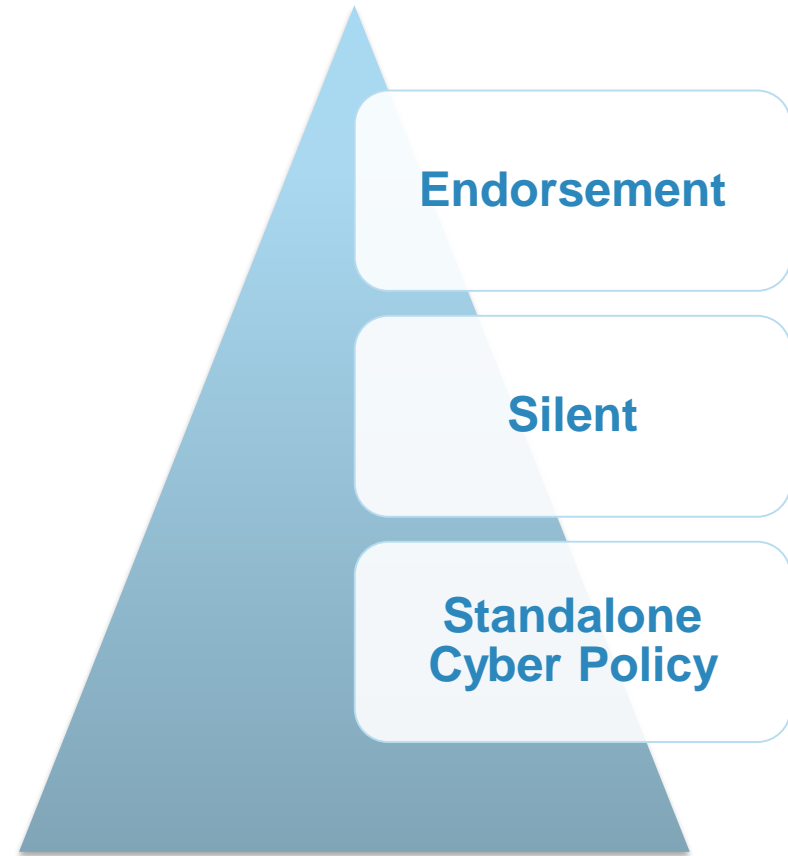
Cyber insurance policies usually provide two main types of coverage

- **First-party coverages** such as costs of recollection, restoration or rebuilding of lost data, cyber extortion, fraud and business interruption (without material damage) following a cyber event.
- **Third-party coverages** including privacy liability arising out of the loss or theft of 3rd party data, liability for any damage caused to third parties due to misuse or breach of security of a company's IT system as well as Internet media liability.

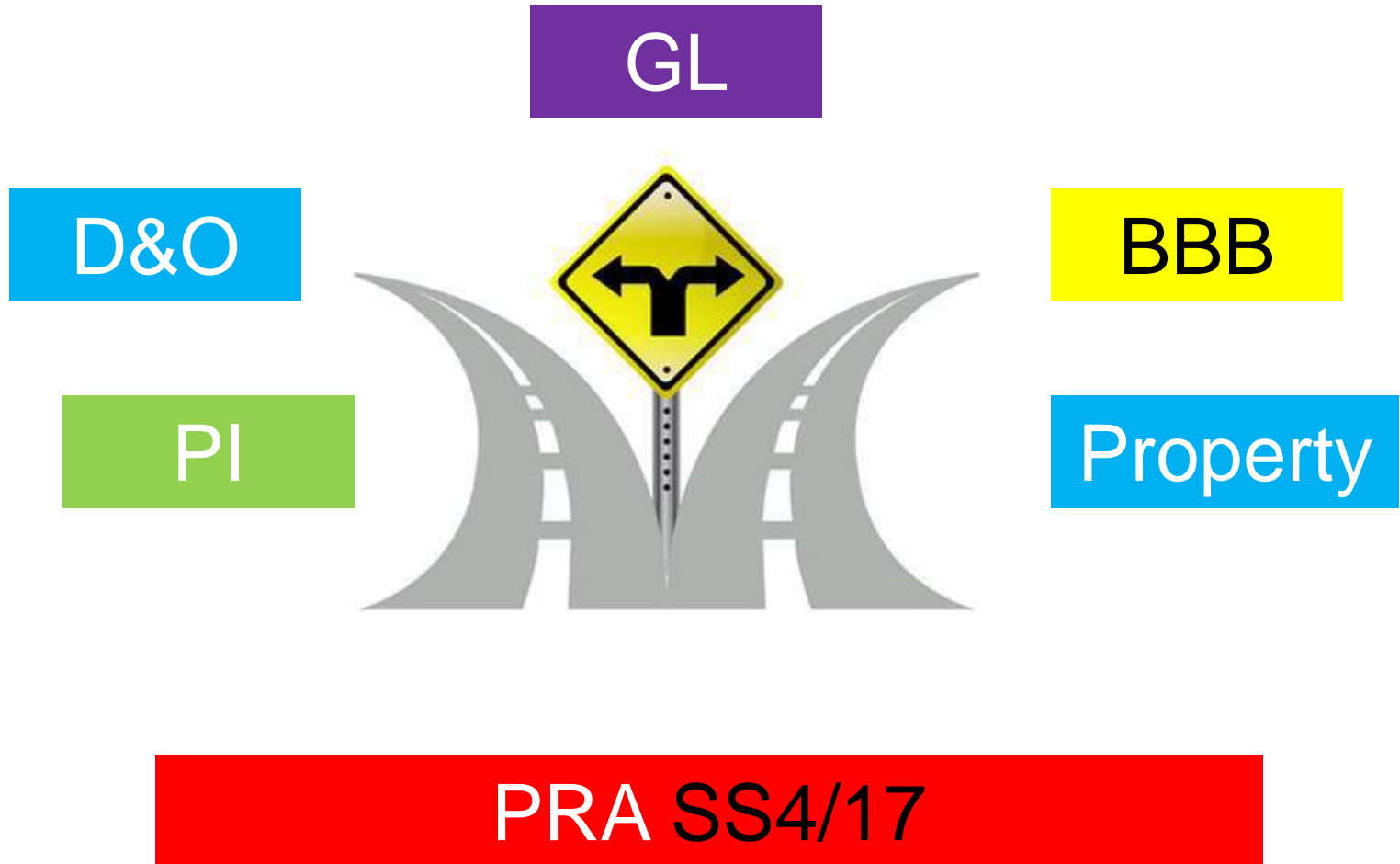


# Existing and future insurance products

- **Standalone:** Industry specific coverage
- **Imbedded into a P&C product:** Attach Cyber endorsement into policies such as Property BI, PI, BBB, Crime etc
- **Silent Cyber**



# Silent Cyber and Untested Policy Wording



# Potential coverage for cyber risk in traditional policies



# CYBER COVERAGE IN CGL POLICIES

Many CGL policies have specific exclusions for electronic data. ISO, an industry organization that develops standard insurance forms, filed a number of data breach exclusionary endorsements for use with its standard-form, excess and umbrella liability policies, which took effect in May of 2014



# CYBER COVERAGE IN CGL POLICIES

Effective May 1, 2014 in many jurisdictions, ISO introduced several endorsements:

- CG 21 06 05 14 (Exclusion – Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability – With Bodily Injury Exception) — excludes coverage, under Coverages A and B, for injury or damage arising out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information.

# CYBER COVERAGE IN CGL POLICIES

- CG 21 07 05 14 (Exclusion – Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability – Limited Bodily Injury Exception Not Included) – which is very similar to CG 21 06 but does not include the bodily injury exception described above.
- CG 21 08 05 14 (Exclusion – Access Or Disclosure Of Confidential Or Personal Information (Coverage B Only) — exclusion with respect to any access to or disclosure of any person’s or organization’s confidential or personal information is limited to personal and advertising injury.

# Sony Case

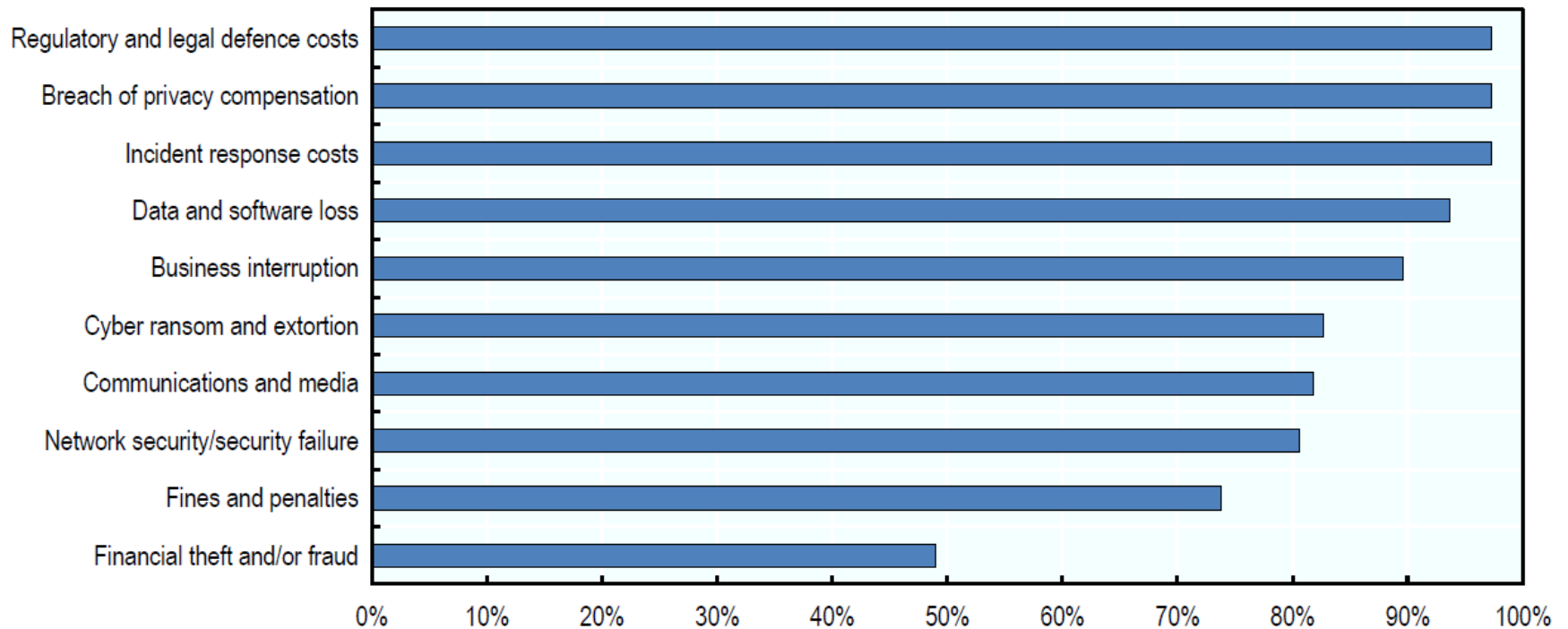
- **Sony**, in one of the larger data breaches in the past, Sony Corporation's popular PlayStation network was hacked in June of 2011
- Exposing the personal information of 77 million user accounts in an incident which appears to have cost Sony US\$2 billion.
- Sony filed for a declaratory judgment that its CGL policy covered costs of the breach.
- The carrier took the position that the CGL policy only covered "property damage" and "bodily injury," neither of which, the carrier contended, had occurred as a result of the breach.
- On February 21, 2014, in what may be a very influential decision, New York Supreme Court Justice Jeffrey K. Oing issued a bench ruling that the policy did not cover breach costs because the provision only covered confidential material published directly by Sony, not by the hackers who stole the information.
- This decision underscores the reason that many more companies are seeking out policies specifically written to cover cyber business interruption, notification, crisis management and liability-related losses.

# Silent cyber risk

- Less is heard though about the so-called silent cyber risk, i.e. insurance policies that don't explicitly include or exclude coverage for cyber risk.
- There are many such policies. For example, any provider of professional or other services, or any manufacturer or distributor of products that carries insurance, could be exposed to cyber risk.
- This silent risk is the main focus of Supervisory Statement SS4/17 issued in July 2017 by the U.K.'s Prudential Regulation Authority (PRA).
- The implications for senior executives of insurance companies of SS4/17 are very significant



# Share of stand-alone cyber policies covering different loss types



Source: OECD's survey report (OECD report for the G7 presidency)

# Cyber Insurance – First Party Loss

<b>First Party</b>	<b>Network business interruption</b>	Loss of income and extra expense resulting from a total or partial failure of by DOS, malicious code, unauthorized access/use to computer system
	<b>Intangible property</b>	Costs to restore or recreate data or software resulting from network security failure
	<b>Loss of Digital Assets</b>	Expenses & costs incurred resulting from damage, alteration, theft, digital assets caused by DOS, malicious code, unauthorized access/use to
	<b>Crisis Management costs</b>	Legal costs to comply with privacy regulations, credit monitoring, PR, costs, resulting from a security data breach, privacy breach or breach of
	<b>Cyber Extortion</b>	Extortion expenses and monies paid resulting from a threat to destroy or assets which are acquired by unauthorized access

# Cyber Insurance – 3<sup>rd</sup> Party Loss

<b>Third Party</b>	<b>Litigation and regulatory</b>	Covers the costs associated with civil lawsuits, judgments, settlements or penalties resulting from a cyber event.
	<b>Regulatory response</b>	Covers the legal, technical or forensic services necessary to assist the policyholder in responding to governmental inquiries relating to a cyber attack, and provides coverage for fines, penalties, investigations or other regulatory actions
	<b>Notification costs</b>	Covers the costs to notify customers, employees or other victims affected by a cyber event, including notice required by law
	<b>Crisis management</b>	Covers crisis management and public relations expenses incurred to educate customers concerning a cyber event and the policyholder's response, including the cost of advertising for this purpose.

Continue..




# Cyber Insurance – 3<sup>rd</sup> Party Loss

..Continue

<b>Third Party</b>	<b>Credit monitoring</b>	Covers the costs of credit monitoring, fraud monitoring or other related services to customers or employees affected by a cyber event.
	<b>Media liability</b>	Provides coverage for media liability, including coverage for copyright, trademark or service mark infringement resulting from online publication by the insured.
	<b>Privacy liability</b>	Provides coverage for liability to employees or customers for a breach of privacy

# Covering Insurance Gaps with Cyber Insurance

	Property	General Liability	Crime	K&R	PI	Cyber
<i>1st Party Data Protection Privacy Risks</i>						
Network Interruption	Yellow	Red	Red	Red	Red	Green
Cyber Extortion	Red	Red	Red	Yellow	Red	Green
Data Restoration, Recollection, Recreation (Determination and Action)	Red	Red	Red	Red	Red	Green
Employee sabotage of Data	Red	Red	Yellow	Red	Yellow	Green
Virus/Hacker damage to Data	Red	Red	Red	Red	Red	Green
Denial of Service attack	Yellow	Yellow	Red	Red	Red	Green
Physical damage to Data Only	Yellow	Red	Red	Red	Red	Yellow




Coverage Provided   
 Coverage Possible   
 No Coverage 

For reference and discussion only: policy language and facts of claim will require further analysis

Slide courtesy of AIG HK

## Covering Insurance Gaps with Cyber Insurance

	Property	General Liability	Crime	K&R	PI	Cyber
<b>3rd Party Data Protection Privacy Risks</b>						
Breach of Personal Information	Yellow	Yellow	Yellow	Red	Yellow	Green
Breach of Corporate Information	Red	Red	Red	Red	Yellow	Green
Outsourcing Liability/Vicarious Liability	Red	Red	Red	Red	Red	Green
Contamination of Third Party Data by any unauthorized software, computer code or virus	Red	Yellow	Red	Red	Yellow	Green
Denial of access to third party data	Red	Red	Red	Red	Yellow	Green
Theft of an access code from the Company's premises	Red	Red	Red	Red	Yellow	Green
<b>Destruction, modification, corruption, damage or deletion of Data</b>	Red	Red	Red	Red	Red	Green
Physical theft of the Company's hardware	Red	Red	Red	Red	Yellow	Green
Data disclosure due to a Breach of Data Security	Red	Red	Red	Red	Yellow	Green
<b>Costs and expenses for legal advice and representation in connection with an Investigation</b>	Red	Red	Red	Red	Yellow	Green
<b>Data Administrative Fines</b>	Red	Red	Red	Red	Yellow	Green
<b>Repair of Company/Individuals Reputation</b>	Red	Red	Red	Red	Yellow	Green
Media Content Liability (IP, Plagiarism, defamation, trespassing)	Red	Yellow	Red	Red	Yellow	Green
<b>Notification Costs</b>	Red	Yellow	Red	Red	Red	Green
Monitoring Costs (with identity theft education and credit file or identity monitoring)	Red	Yellow	Red	Red	Red	Green

Coverage Provided   
 Coverage Possible   
 No Coverage 

For reference and discussion only: policy language and facts of claim will require further analysis

Slide courtesy of AIG HK

# Cyber Insurance – Typical 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 that happened before the inception date, if the Insured knew or could have reasonably foreseen
- **Bodily Injury**
- **Property Damage:** No cover for hardware, but restorage expense for data and computer programs that exists in computer system is covered
- **Failure in power, telecommunications other infrastructure:** No cover for infrastructure failure unless under the Insured's operational control

# Cyber Insurance – Typical Exclusions

...Continue

- NAT CAT or any other physical event
- Act of Terrorism, war, invasion
- Fine or Penalty arising out of Payment Card Industry Standard/Payment Card Company Rules
- Infringement of any patent or trade secret by Insured, Insured former employee
- Unlawful collection of personally identifiable non public information by Insured
- Theft, Loss of unencrypted Lap tops and mobiles

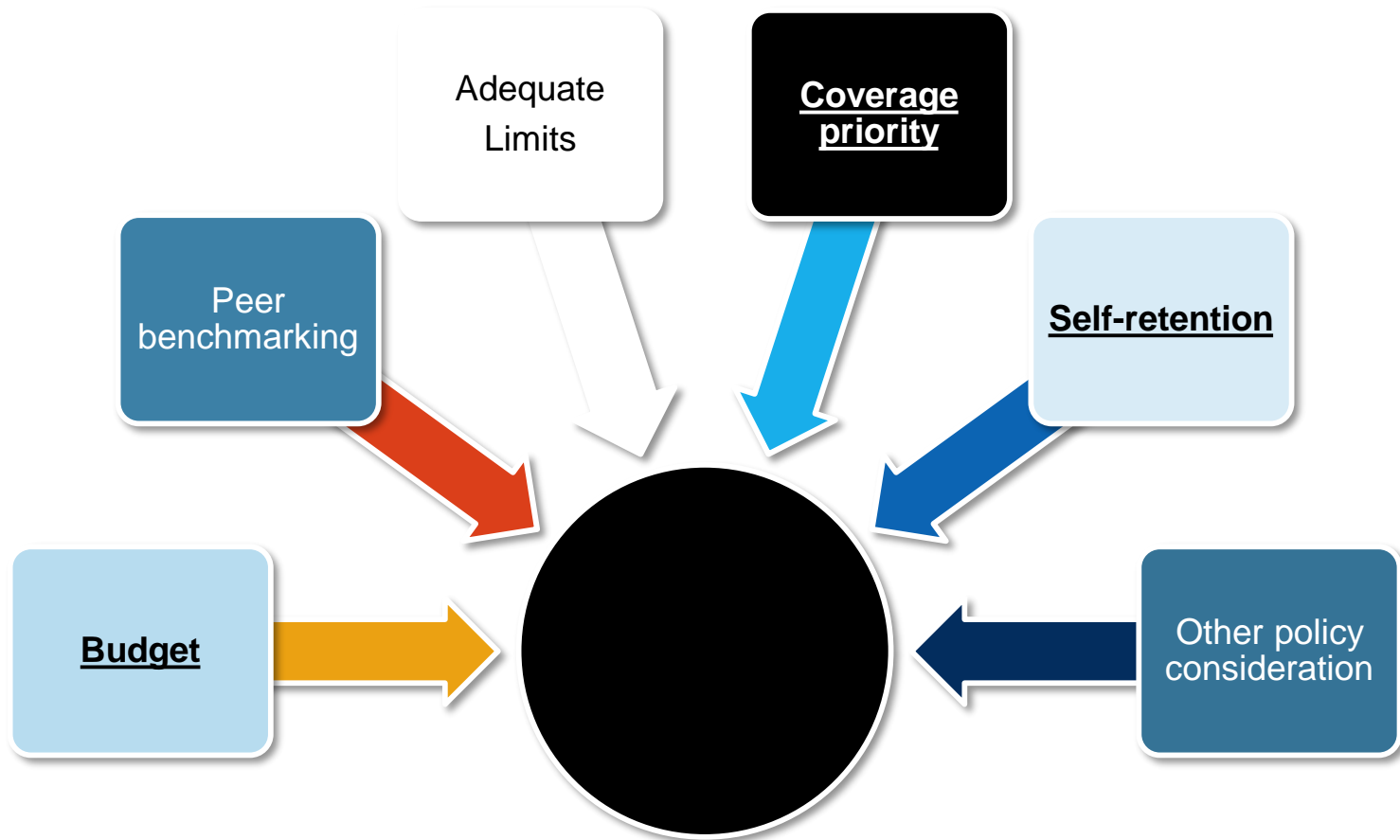


## Most vulnerable industries in Asia

*Within Asia, FireEye Labs identified the following industries as having experienced advanced persistent cyber-attacks during 2013, in order:*

- Financial Services
- Government (Federal)
- High-Tech
- Chemicals / Manufacturing / Mining
- Services / Consulting
- Higher Education
- Telecom (Internet, Phone and Cable)
- Energy / Utilities / Petroleum
- Entertainment / Media
- State and Local Government

# Client considerations





# Underwriting

# UW Information: Current method

## Industry



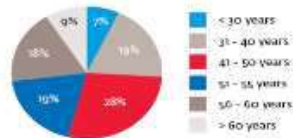
## Recovery Plan



## Demography



Age distribution of employees



## Revenue



## Security



**BITSIGHT**

## UW Information: *The insured's industry*

Some industries have more significant exposure to PHI or PII. For example, companies in the healthcare industry are likely to have PHI. In the retail industry, companies might be further subcategorized based on characteristics such as the number of credit card transactions processed yearly.



## UW Information: *Geographic spread of operations*

Companies with a global footprint face different risks in different jurisdictions. The US is a fairly litigious environment with significant privacy laws and regulations, creating significant exposure. Other jurisdictions may not have robust regulation or enforcement, reducing the risk of exposure from a breach.



## UW Information: *Security and privacy controls*

- Companies that can demonstrate high quality controls will generally see lower premiums.
- Notably, quality is not based solely on the technology a company uses to protect data. Rather, quality is the combination of people, processes and technology that a company uses to safeguard PHI and PII.
- While some insurers continue to inflict lengthy applications on applicants, much more commonly carriers ask the company to participate in a briefing at which individuals with responsibility for management and security of PHI and/or PII provide information and respond to questions.

Security



**BITSIGHT**

## UW Information: *Data breach team choice*

- If the insured wants to utilize its own data breach team rather than using the carrier's team, the premium will likely increase.
- Policies requiring the insured to use the carrier's data breach team reflect the savings a carrier is able to realize as a result of providing high volume business to chosen experts.
- Some carriers will not write a policy that permits the insured to choose its own data breach team.





# Future of Underwriting

## Data Sources

Public Data

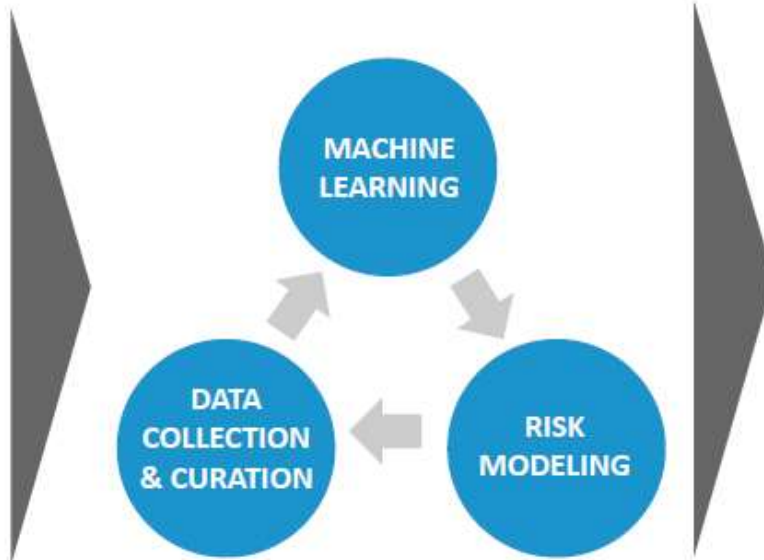
Open Source Data

Proprietary Data

Customer Data

3<sup>rd</sup> party Data

## Data Listening and Risk Analytics



## Application Framework

**Cyber Insurance**

Underwriting

Pricing

Accumulation

# Cyber Pricing Techniques

## It is a Different Ballgame

- Data issue
- No Geographical Limitation
- Network Risk
- Significance of the Human Element
- Correlation of Attacks
- Definition of a Cyber Cat
- Technology Evolution
- Silent Coverage

## Accumulation of risks

- Cyber is more unusual, more uncertain and more potentially dangerous for the insurance industry than new offerings of the past.
- Probabilistic Cyber Model
- Lloyd's blackout model



## Reinsurers' perspective.

- Cyber is top concern for reinsurers today

<b>Reinsurers' Banana Skins 2017</b>	<b>Reinsurers' Banana Skins 2015</b>
1) Cyber risk (3)	1) Market conditions
2) Change management (-)	2) Regulation
3) Investment performance (8)	3) Cyber risk
4) Macro-economy (10)	4) Interest rates
5) Technology (-)	5) Natural catastrophes
6) Competition (-)	6) Distribution channels
7) Political interference (-)	7) Guaranteed products
8) Interest rates (4)	8) Investment performance
9) Regulation (2)	9) Quality of risk management
10) Cost reduction (-)	10) Macro-economy

Source: PWC report



## Cyber Risk Management and Assessment

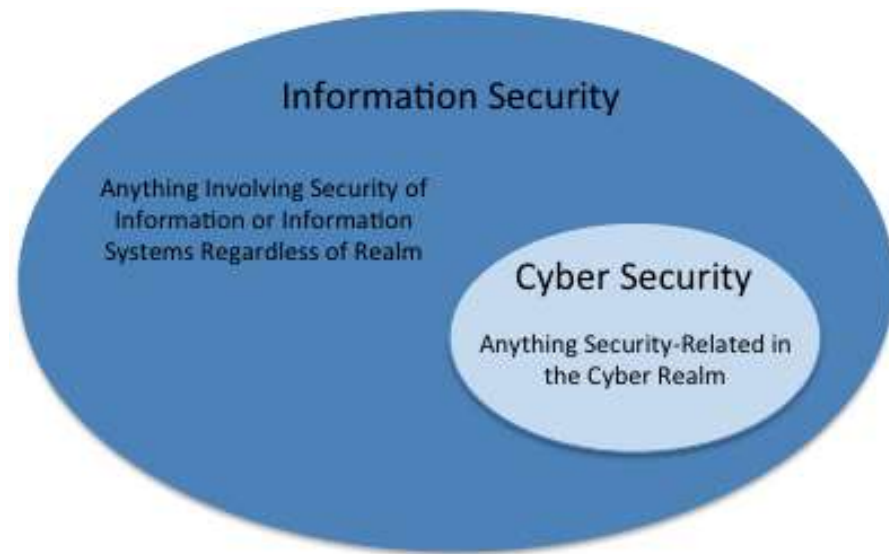
# Definitions

## — Information Security

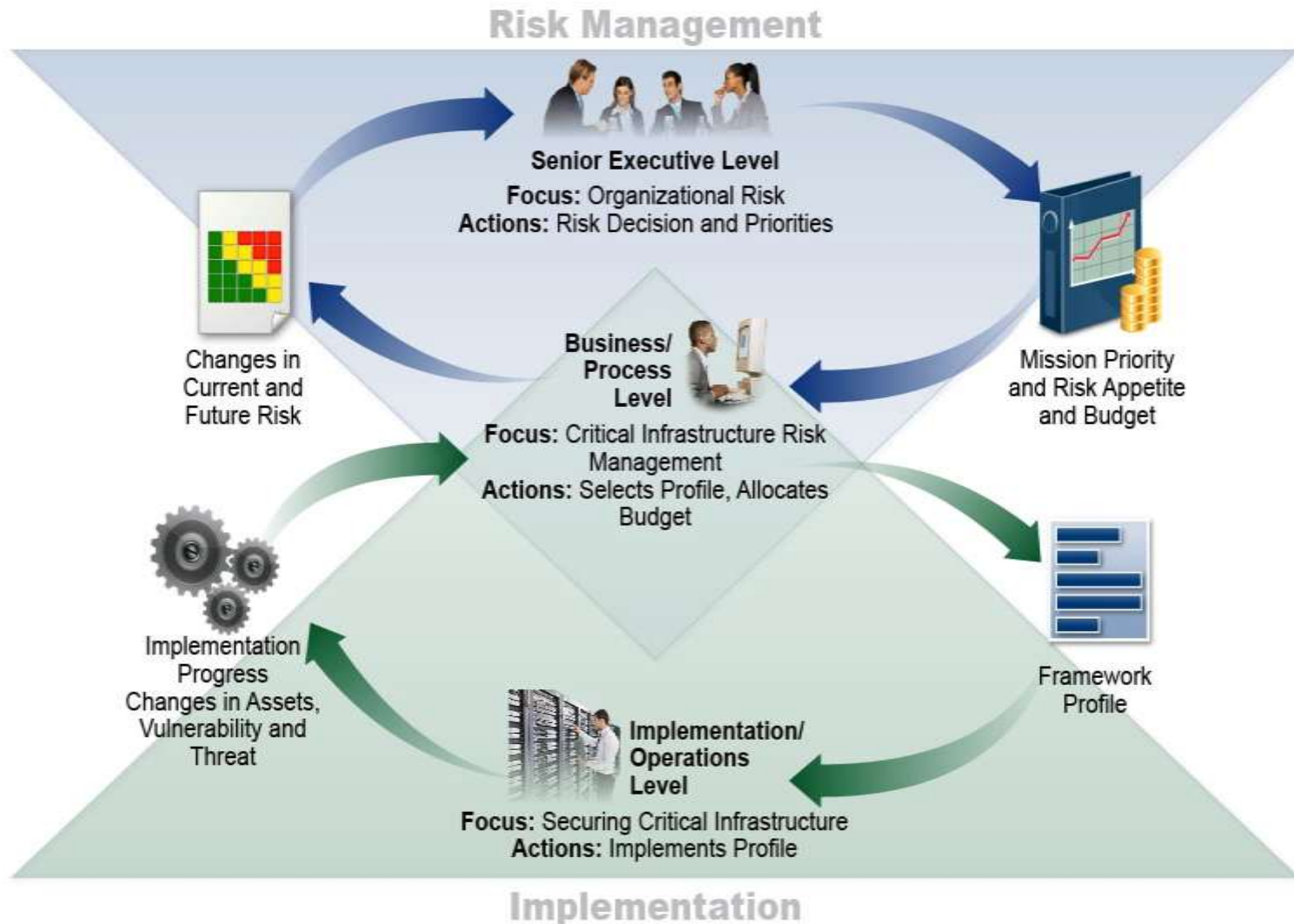
The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

## — Cybersecurity

The ability to protect or defend the use of cyberspace from cyber attacks

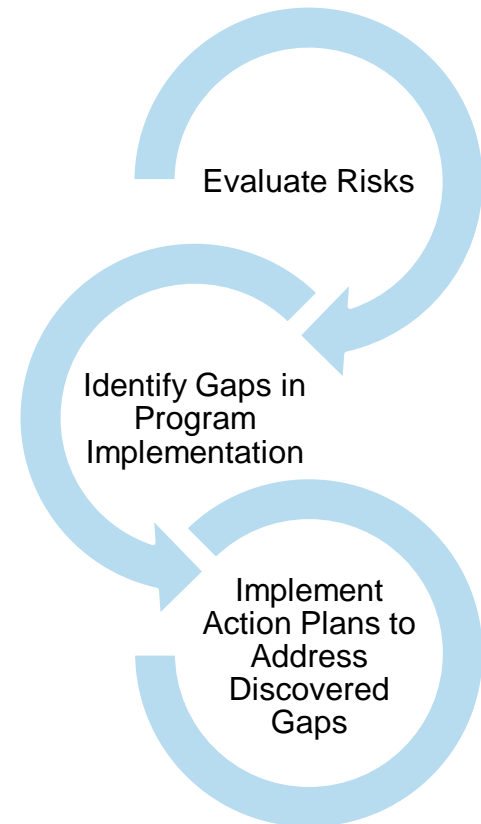


# Risk Management



# Cybersecurity Best Practices

- Continuous Risk Management
  - Not meant to just be a point in time
  - Create a risk strategy that works your firm
  - Remediate! You do not have to fix everything, but develop a plan for addressing gaps





# Cyber Security Risk Assessment Tools

- Industry specific Cyber Risk Assessment Tools
- Industry specific guidelines



# Example: FFIEC Cybersecurity Assessment Tool

- In June 2015, the FFIEC (the Federal Financial Institutions Examination Council) created the Cybersecurity Assessment Tool to help financial institutions evaluate their overall cyber risk
- The tool is an extensive self-assessment questionnaire in PDF form
- Financial institutions are encouraged to continuously assess and monitor their cybersecurity preparedness using the tool

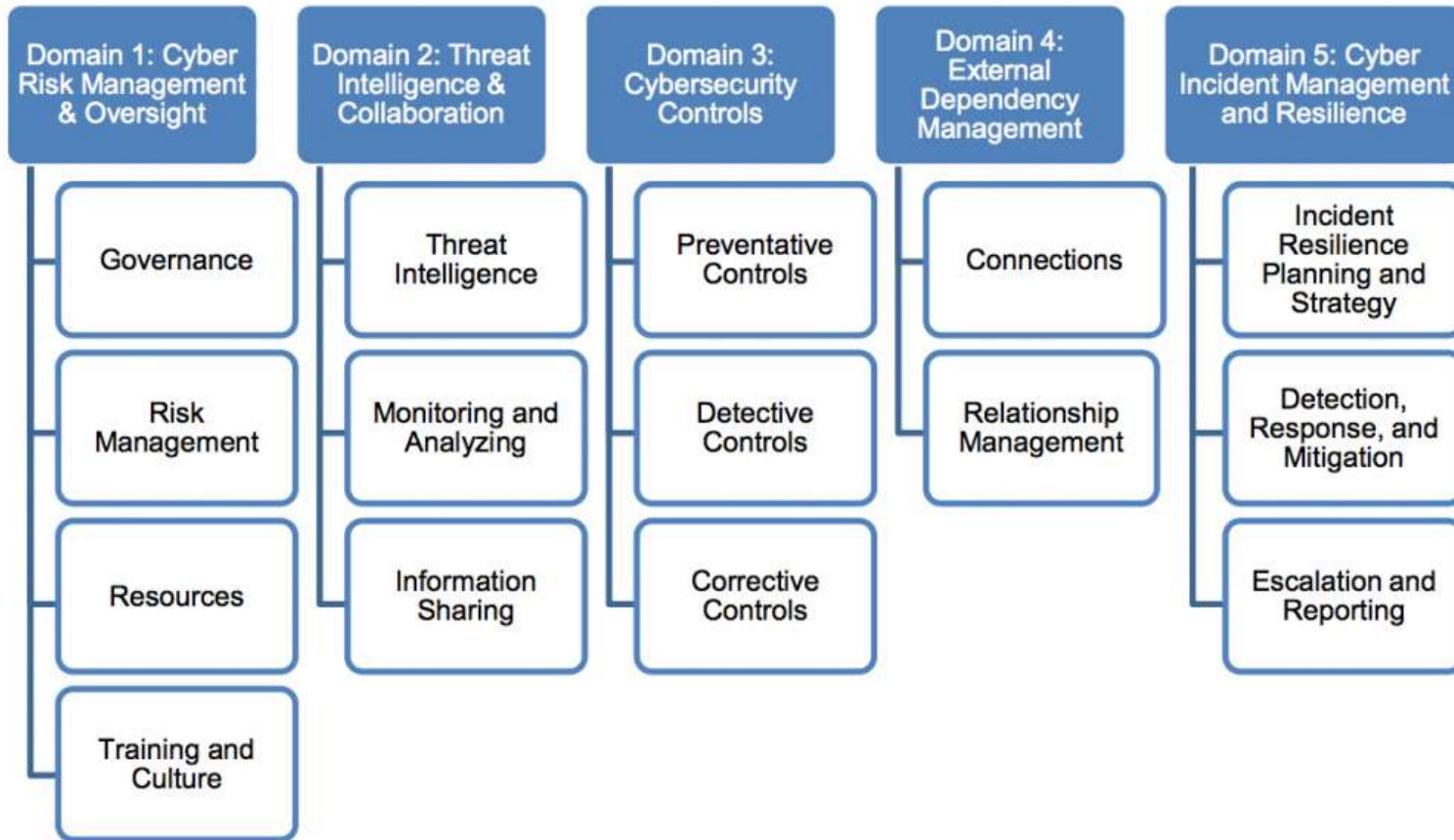


# FFIEC Cybersecurity Assessment Tool

## Inherent Risk Profile

Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Total number of Internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)
Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)
Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)
Personal devices allowed to connect to the corporate network	None	Only one device type available; available to <5% of employees (staff, executives, managers); e-mail access only	Multiple device types used; available to <10% of employees (staff, executives, managers) and board; e-mail access only	Multiple device types used; available to <25% of authorized employees (staff, executives, managers) and board; e-mail and some applications accessed	Any device type used; available to >25% of employees (staff, executives, managers) and board; all applications accessed

# FFIEC Cybersecurity Assessment Tool

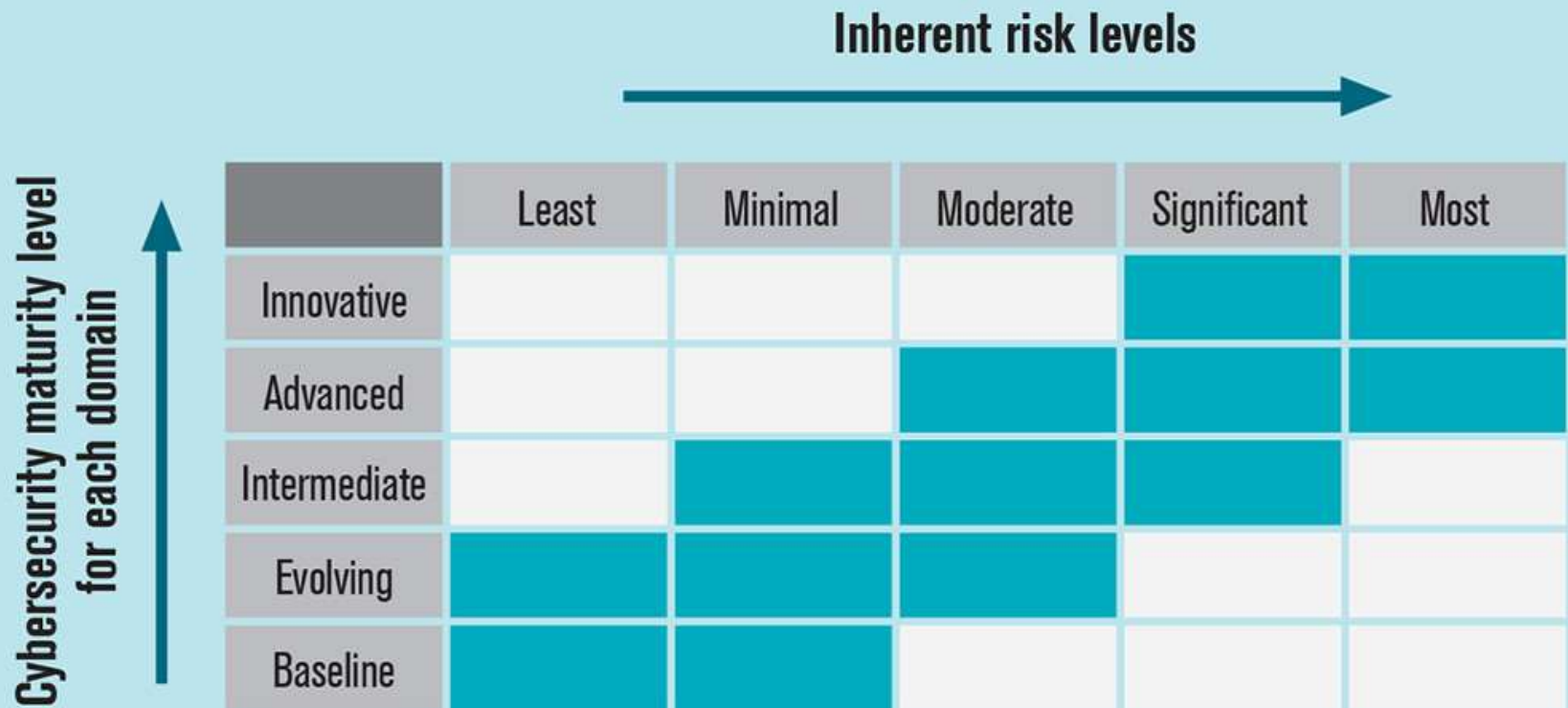


# FFIEC Cybersecurity Assessment Tool



# FFIEC Cybersecurity Assessment Tool

## Cybersecurity Risk/Maturity Relationship



Source: FFIEC Cybersecurity Assessment Tool User's Guide (June 2015)



Claims & Incident Response Service

# When the breach occurs

- Gather details of the incident
- Determine insuring agreements, limits, and retentions that will apply
- What triggers a loss or claim under the policy?
- What are the notice requirements?
- Timing around an upcoming policy renewal/expiring policy period that require an expedited notice?





# Insurers and Reinsurers blame game



# Incident Response

- Incident Response Team
- Reporting & Tracking
- Breach Assessment
  - Notification Requirements
- Law Enforcement
- Disaster and Contingency Planning



## Cyber Placement Strategy

# Placement Consideration

- **Lead** Vs **Follow**
- Trade off between **Underwriting Pen** & **Claim handling services**
- **24/7** hotline
- **“Reinsurer”** Vs **“Direct insurer”**
- **Co-reinsurance** or **layer**





**Questions** |