MARSH

LEADERSHIP, KNOWLEDGE, SOLUTIONS...WORLDWIDE.

# SINGAPORE HEALTHCARE ENTERPRISE RISK MANAGEMENT CONGRESS 2014
# - Data Breach : The Emerging Threat to Healthcare Industry

MARSH & McLENNAN COMPANIES

# DATA BREACH – A FICTIONAL CASE STUDY
# THE FIRST SIGNS OF TROUBLE

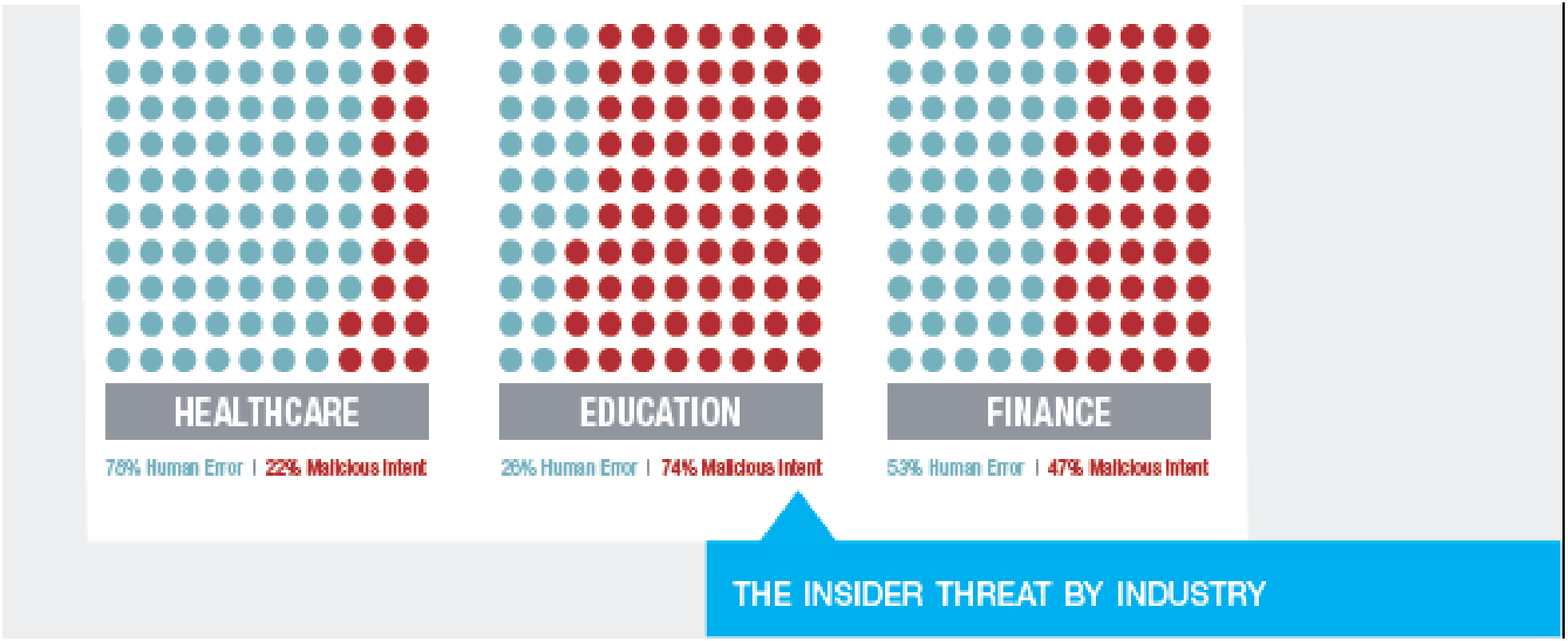
- Friday, 5.20 pm : an employee of the IT Dept called the company hotline about a possible intrusion of the computer system of the hospital
- 6 pm : The system triggered an alert and on further investigation, the intrusion was isolated to 2 servers within the computer system
- 8 pm : The servers were identified to be a repository of medical records of patients at the hospital from 2012 – 2013
- 9 pm : It was estimated that there are 10,000 medical records in the 2 servers
- 11 pm : A HR employee reported that a laptop containing the information of the hospital's staff (including payroll) has been accidentally left on a taxi

# DATA BREACH & HEALTHCARE INDUSTRY – THE FACTS

- 2013 Kroll Survey of clients in the USA
  - Top 3 cyber targets in 2013 are
  - Healthcare, Higher Education and Finance
- Healthcare  surveyed at 38%
- Educational institutions at 13%
- Financial services at 9%

# DATA BREACH – IS THIS A REAL THREAT?
# KROLL 2013 CYBER SURVEY

- Risk of human error causing data breach is highest for healthcare industry
- Malicious intent is lowest compared to higher education and financial services



# DATA BREACH : 1 OF 15 Fifteen Global Risks of Highest Concern World Economic Forum 2014

| Number | Global Risk | Type |
|---|---|---|
| **1** | Fiscal crises | |
| **2** | Unemployment and underemployment | |
| **3** | Water crises | |
| **4** | Income disparity | |
| **5** | Climate change | |
| **6** | Extreme weather events | |
| **7** | Global governance failure | |
| **8** | Food crises | |
| **9** | Failure of financial mechanism or institution | |
| **10** | Political and social instability | |
| **11** | **Cyber attacks** | |
| **12** | Interstate conflict | |
| **13** | Terrorist attack | |
| **14** | State collapse | |
| **15** | Natural catastrophe | |

Respondents were asked to provide the five risks of highest concern globally

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

Source: World Economic Forum, Global Risks 2014

# HEALTHCARE INDUSTRY
# REAL DATA BREACH INCIDENTS

- Computer stolen from a hospital contained index of more than 500,000 patients dating from the 1980s
  - Index information includes name, age, DOB, medical record number and social security number.
- 8 computers where stolen from a company which handles medical billing and collections for a county
  - 342,000 patients were affected because their names, addresses and billing information were stored in those computers.
- More than 200 hard drives belonging to a regional healthcare authority were sent for safe disposal but an employee of the company extracted medical records of thousands of patients and sold them online
  - the data included the HIV test results carried out by the regional healthcare authority
- Personal information of 600,000 patients were stolen from a health insurer

# DATA BREACH : WHAT IS AT RISK?

## Consumer Information

- Credit Cards, Debit Cards, and other payment information
- Social Security Numbers, ITIN's, and other taxpayer records
- Customer Transaction Information, like order history, account numbers, etc.
- Protected Healthcare Information (PHI), including medical records, test results, appointment history
- Personally Identifiable Information (PII), like Drivers License and Passport details
- Financial information, like account balances, loan history, and credit reports
- Non-PII, like email addresses, phone lists, and home address that may not be independently sensitive, but may be more sensitive with one or more of the above

## Employee Information

- Employers have at least some of the above information on all of their employees

## Business Partners

- Vendors and business partners may provide some of the above information, particularly for Sub-contractors and Independent Contractors
- All of the above types of information may also be received from commercial clients as a part of commercial transactions or services
- In addition, B2B exposures like projections, forecasts, M&A activity, and trade secrets

**Many people think that without credit cards or PHI, they don't have a data breach risk. But can you think of any business *without* any of the above kinds of information?**

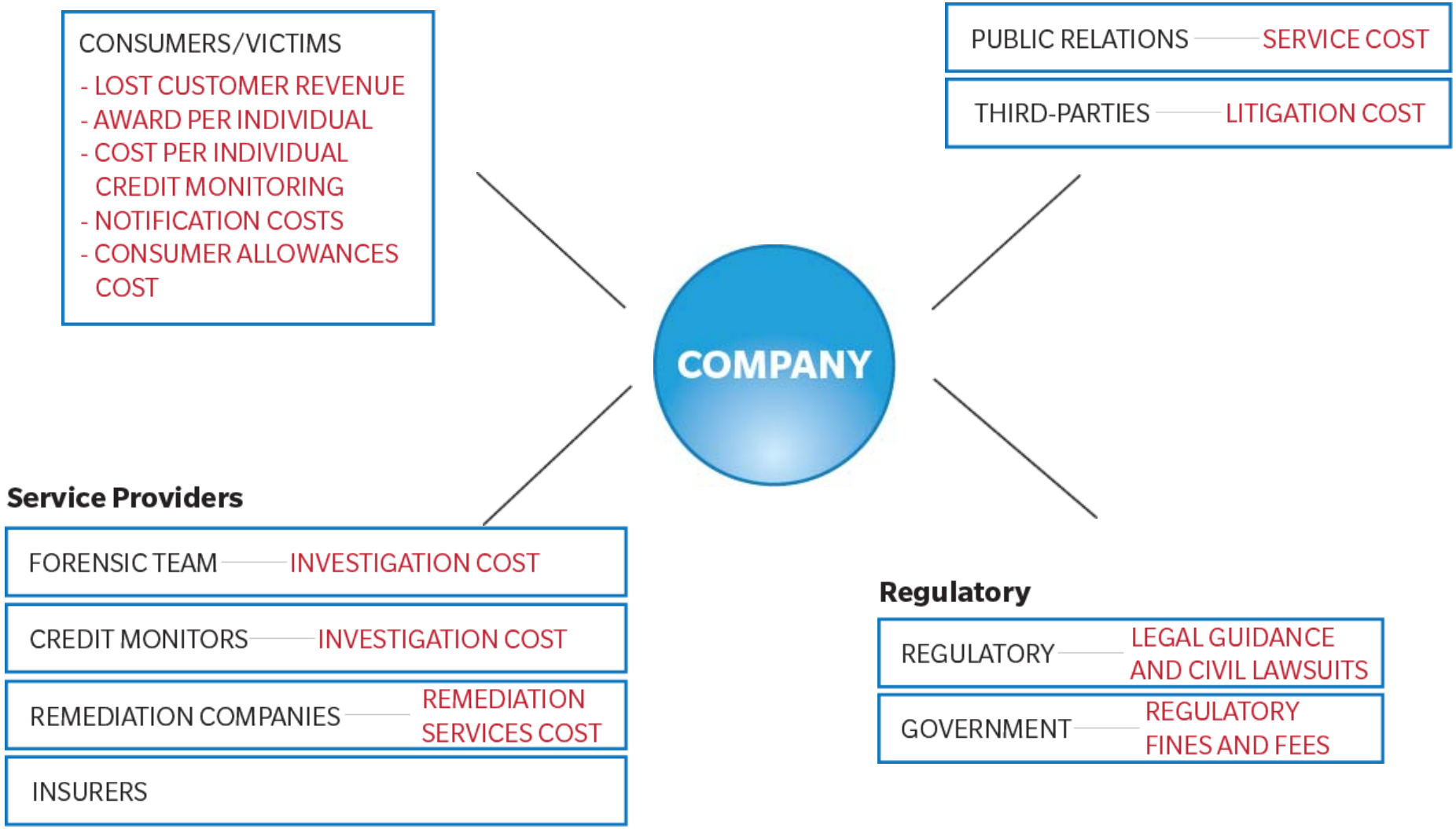
# DATA BREACH : CAUSES AND THREATS

- Internal
  - Rogue employees
  - Careless staff
- External
  - Organized crime
    - Foreign
    - Domestic
  - Hackers/Hacktivists
- Technology
  - Hackers, viruses, SQL Injections, etc…
  - Structural vulnerability
  - Social Media/Networking
  - Phishing
- Old school
  - Laptop theft
  - Dumpster diving
- Regulatory
  - HIPAA, HITECH, Red Flags
  - FTC, HHS, state attorney generals
  - 47 State Breach notification laws
  - Foreign Laws: Canada, South Korea, Spain

# DATA BREACH
# WHAT ARE THE IMPLICATIONS**?**

- Legal liability to others for computer security breaches
- Legal liability to others for privacy breaches of confidential information
- Regulatory actions, fines and scrutiny
- Cyber-extortion
- Cyber-terrorism
- Loss or damage to data / information
- Loss of revenue due to a computer attack
- Extra expense to recover / respond to a computer attack
- Loss or damage to reputation

# DATA BREACH
# WHO IS INVOLVED? STAKEHOLDERS



# DATA BREACH : DIAGNOSIS AND RESPONSE

## Discovery

**Actual or alleged theft, loss, or unauthorized collection/disclosure of confidential information that is in the care, custody or control of the Insured, or a 3rd for whom the Insured is legally liable.**

**Discovery can come about several ways:**

- **Self discovery: usually the best case**
- **Customer inquiry or vendor discovery**
- **Call from regulator or law enforcement**

## First Response

**Forensic Investigation and Legal Review**

- **Forensic tells you what happened**
- **Legal sets out options/obligations**

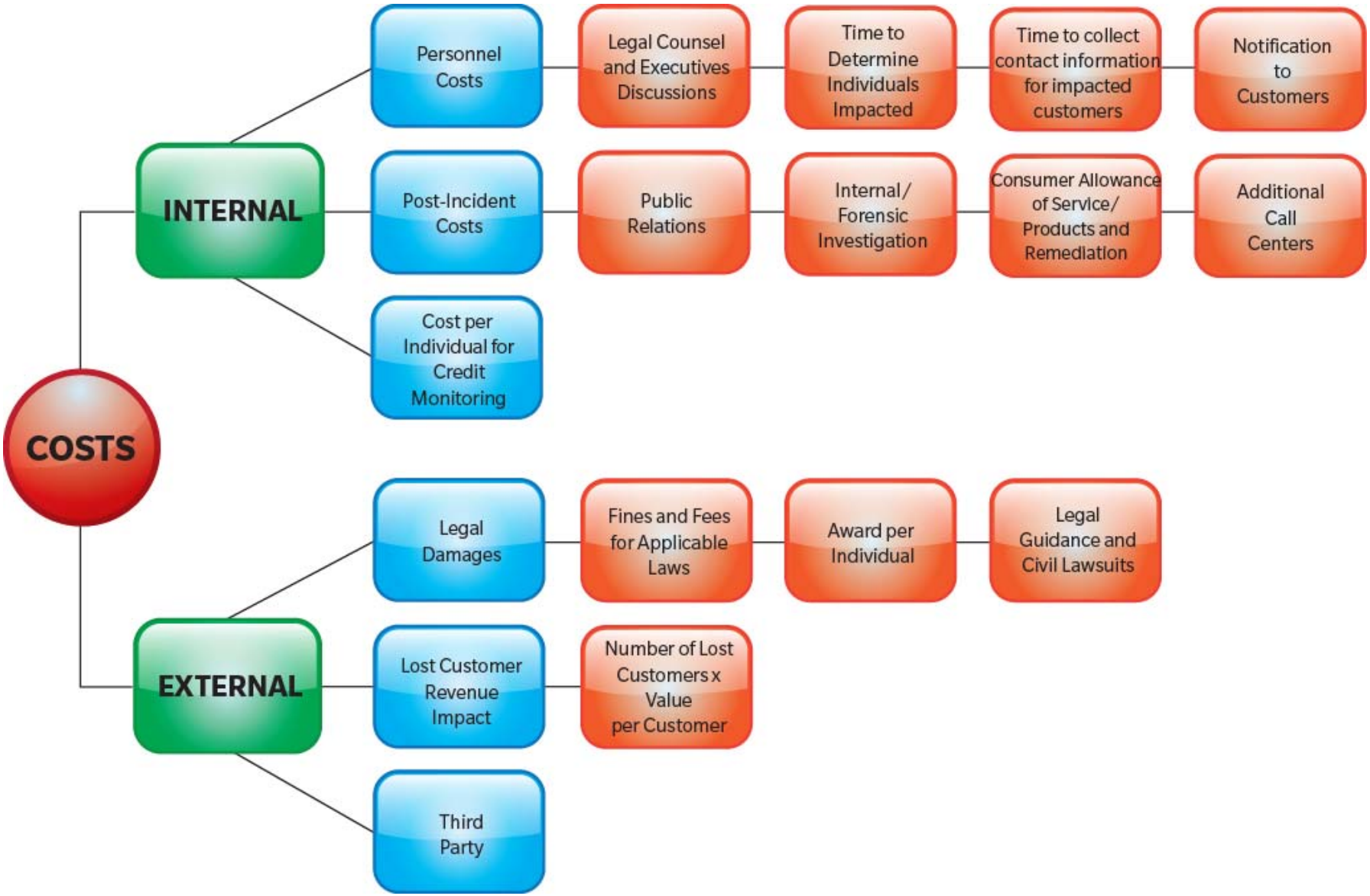
## External Issues

- **Public Relations**
- **Notification**
- **Remedial Service Offering**

## Long-Term Consequences

- **Income Loss**
- **Damage to Brand or Reputation**
- **Regulatory Fines, Penalties, and Consumer Redress**
- **Civil Litigation**

# DATA BREACH : TYPES OF COSTS INVOLVED



# DATA BREACH : THE GLOBAL PERSPECTIVE

**Norton Report – The global cost of cyber crime**

- $113 global cost of consumer cyber crime
- $298 per victim cost (up 50% on 2012)
- 378M victims per year or 12 every second

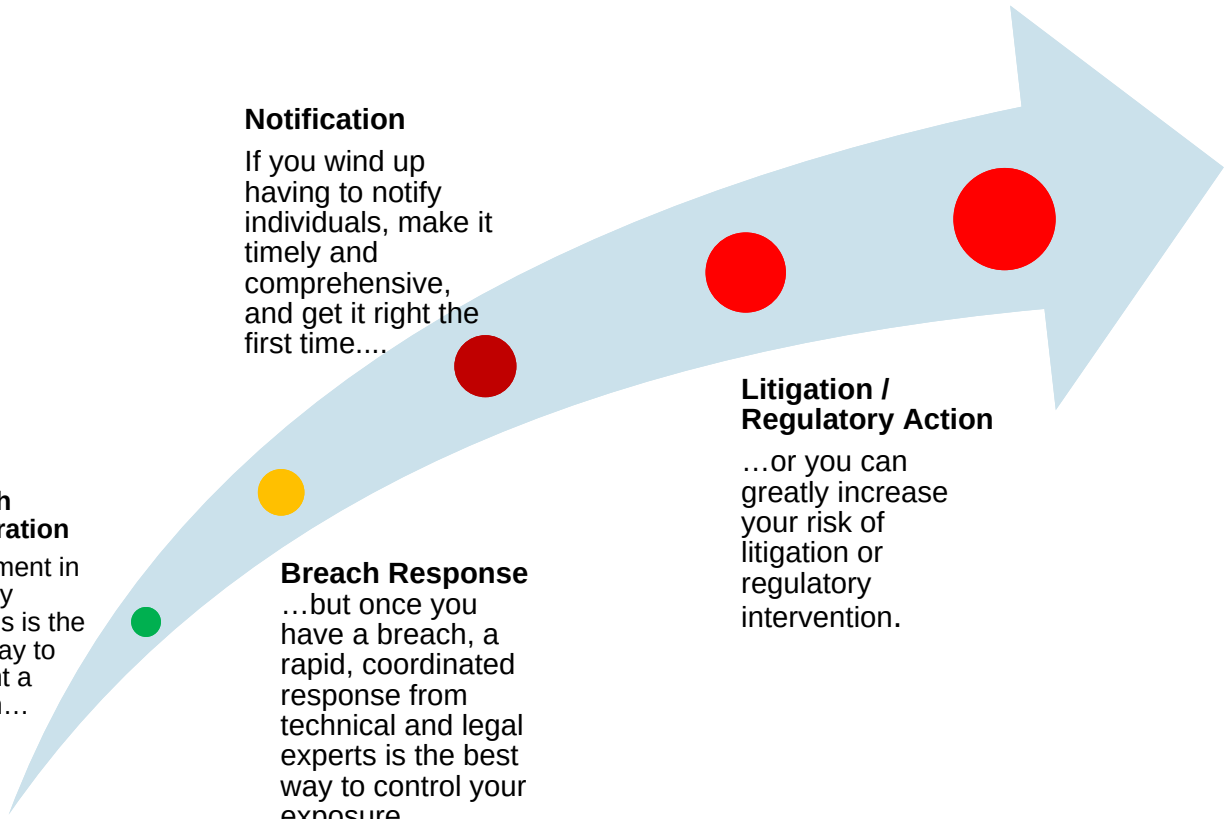
**McAfee Report – The global cost of cybercrime and cyber espionage**

- $300M - $1BN cost from global cyber activity

**Ponemon Global Report – Cost of a data breach study**

- Of 9 countries included the US had the highest cost of a data breach at $5.4M. India was the lowest at $1.1M
- Of 9 countries included Germany had the highest per capita cost at $199 and India the lowest at $42.

# DATA BREACH RESPONSE : TIME IS OF THE ESSENCE!



**Breach Preparation**

Investment in security controls is the best way to prevent a breach…

**Breach Response**

…but once you have a breach, a rapid, coordinated response from technical and legal experts is the best way to control your exposure.

**Notification**

If you wind up having to notify individuals, make it timely and comprehensive, and get it right the first time....

**Litigation / Regulatory Action**

…or you can greatly increase your risk of litigation or regulatory intervention.

**Reputation and Lost Income**

The ultimate goal is to preserve corporate reputation and get the business back to normal as quickly as possible. The most effective management of this risk comes from effectively handling the earlier risks!

# DATA BREACH : CYBER INSURANCE AS A REMEDY
## GENERAL COVERAGE

- Business Interruption
- Crisis Management

- Data Loss & System Damage
- Content Liability
- Online Media Activity Liabilities

- Notification Expenses
- Regulatory Liability

**Cyber Risk Insurance**

# DATA BREACH : CYBER INSURANCE AS A REMEDY
## GENERAL COVERAGE (I)

| | |
|---|---|
| **Network security liability:** | Liability to a third party as a result of<br>• destruction of a third party's electronic data<br>• your networks participation in denial of service attacks<br>• transmission of viruses to third-party computers and systems. |
| **Data privacy liability:** | Liability to a third party as a result of<br>• unauthorized disclosure of personally identifiable information<br>• unauthorized disclosure of third party corporate information<br>Regulatory action arising from the violation of privacy law<br>Cover for your vicarious liability where a vendor loses information you had entrusted to them in the normal course of your business. |

# DATA BREACH : CYBER INSURANCE AS A REMEDY
## GENERAL COVERAGE (II)

| | |
|---|---|
| **Crisis management and identity theft response fund:** | Expenses to respond to a breach event, including:<br>• computer forensic costs<br>• notification costs including call center costs<br>• credit monitoring and ID theft protection costs<br>• public relations and crisis management consultancy costs |
| **Cyber extortion:** | A genuine threat to the computer network or data lead to payment of:<br>• expert fees to negotiate with the hacker<br>• a ransom |
| **Network business interruption:** | The interruption or suspension of computer systems results in:<br>• your loss of income<br>• extra expense incurred to mitigate an income loss<br>Resulting from:<br>• a network security breach.<br>• a network failure.* |

*Specific insurers. Only available in the London Market.

# DATA BREACH : CYBER INSURANCE AS A REMEDY
## GENERAL COVERAGE (III)

| | |
|---|---|
| **Data asset protection:** | The corruption, destruction of data or computer programs, incurs:<br>• replacement, restoration or rectification costs<br>• costs to determine that data or programs can not be replaced |
| **Multimedia liability:** | Liability arising from online content, arising from:<br>• infringement of intellectual property rights<br>• invasion of privacy<br>• defamation<br>• negligent publication or misrepresentation |

# DATA BREACH IS NOT AN I.T. ISSUE!
# FTSE 350 Cyber Governance Health Check - Tracker Report key findings

## Boards are showing an increasing interest in the impact of cyber risk

### A SERIOUS ISSUE

64% of Chairs think their Board colleagues take cyber risk very seriously.

### CYBER SAVVY BOARDS

Most Chairs think their Boards are qualified, to some extent, to manage innovation and risk in a digital age.

2% indicated their colleagues were 'barely qualified'

36% think they have 'good skills'

11% think they are well positioned for the digital age

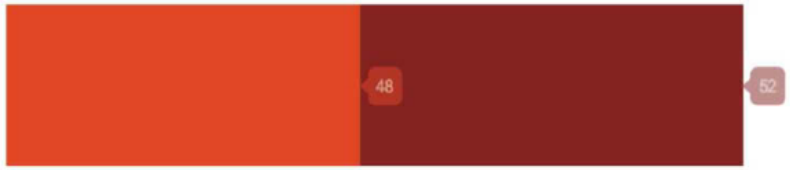
### CYBER IS A BUSINESS RISK

56% of respondents said their strategic risk register includes a cyber risk category.

## Boards are underserved in the provision of good risk analytics

### THE IMPACT OF A CYBER ATTACK

Less than half of FTSE 350 Chairs think their main Board has a clear understanding of the potential impact of information and data asset losses.




### UNDERSTAND THE THREAT

40% of Chairs said the main Board does not receive regular threat intelligence from their CIO or Head of Security.


### WHO HAS YOUR KEY DATA ASSETS?


A quarter of respondents said the main Board has a poor understanding of where the company's key information or data assets are shared with third parties (e.g. suppliers, advisors, customers and outsourcing partners).

# DATA BREACH – AN EMERGING RISK CONTAGION

*"An organization's data breach universe is defined by every individual whose information has been collected and every organization that data has been shared with or accessed by. Therefore, the business' risk of a data breach is limitless, and the consequences far reaching"*

***- Robert Parisi, Marsh FINPRO Network and Security Practice Leader***


Company Registration Number: 197200396D