MARSH

Cyber Security Insurance Solutions

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

MARSH & McLENNAN COMPANIES

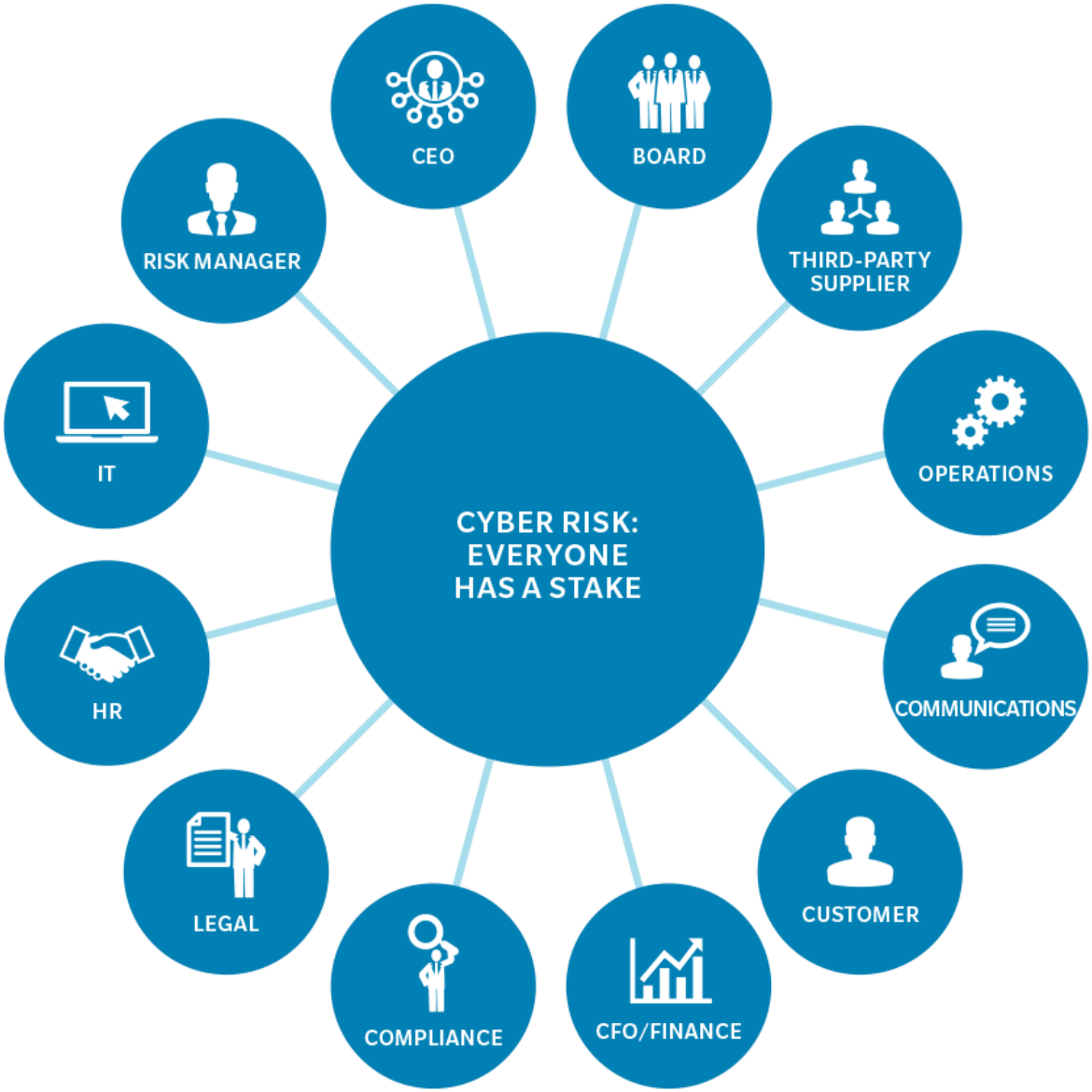
Agenda

- Overview
- Solutions & Approach
- Policy Terms and Conditions
- Comprehensive Crime vs. Cyber

Overview

Cybersecurity is no longer just an IT department issue…

What Is The Impact Across An Organization?



How Do Cyber Risks Impact An Organization?

Operational Disruption

Employee Exposures

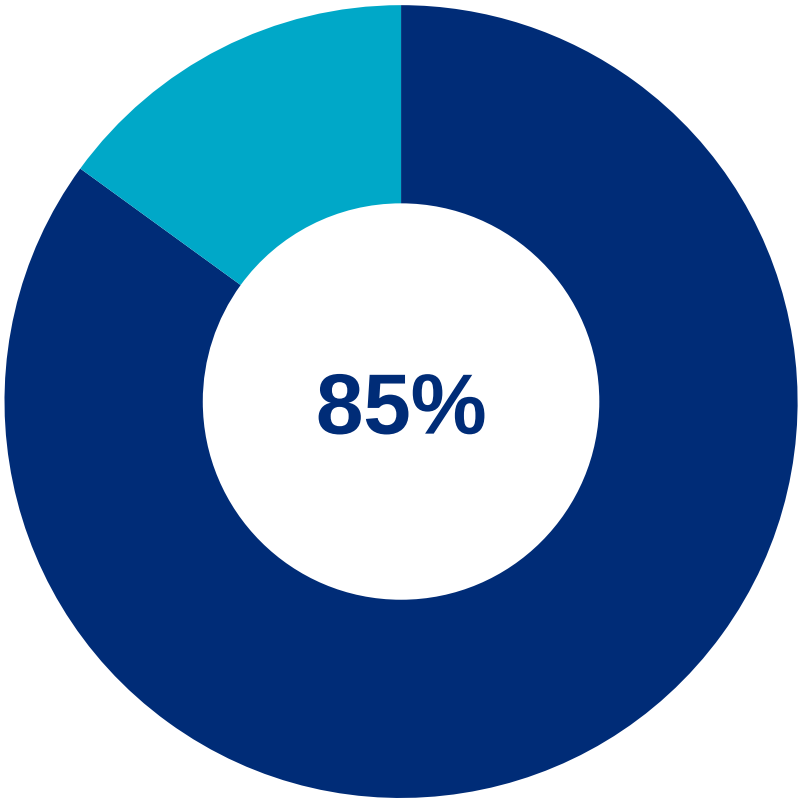
Lawsuits and Reputational Harm

Regulatory and Legal Implications

What Are The Cyber Statistics?

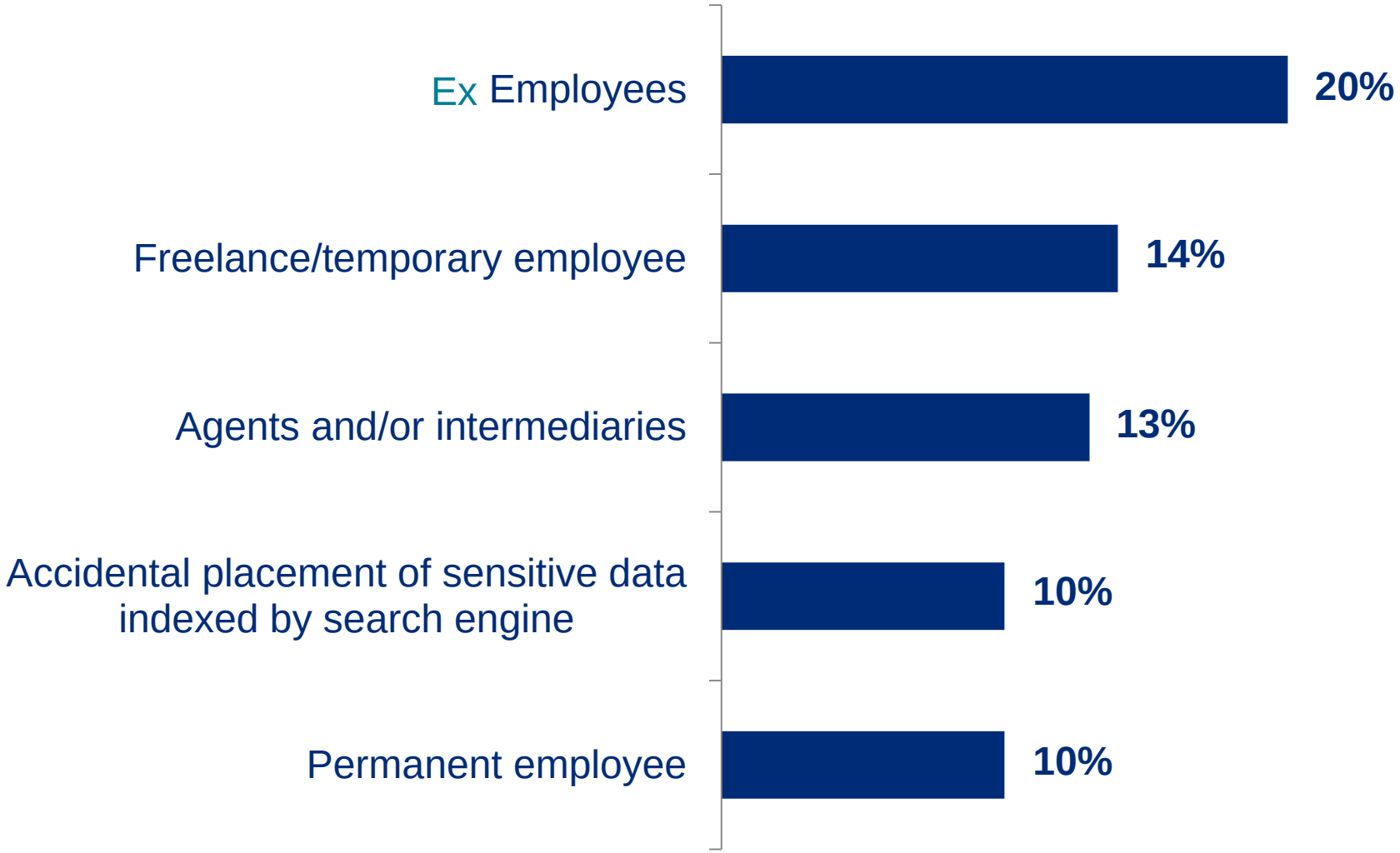
Source: 2016/2017 Global Fraud & Risk Report – Kroll

The number of executives who said that their company experienced a cyber attack, information theft, loss or attack in the last 12 months.

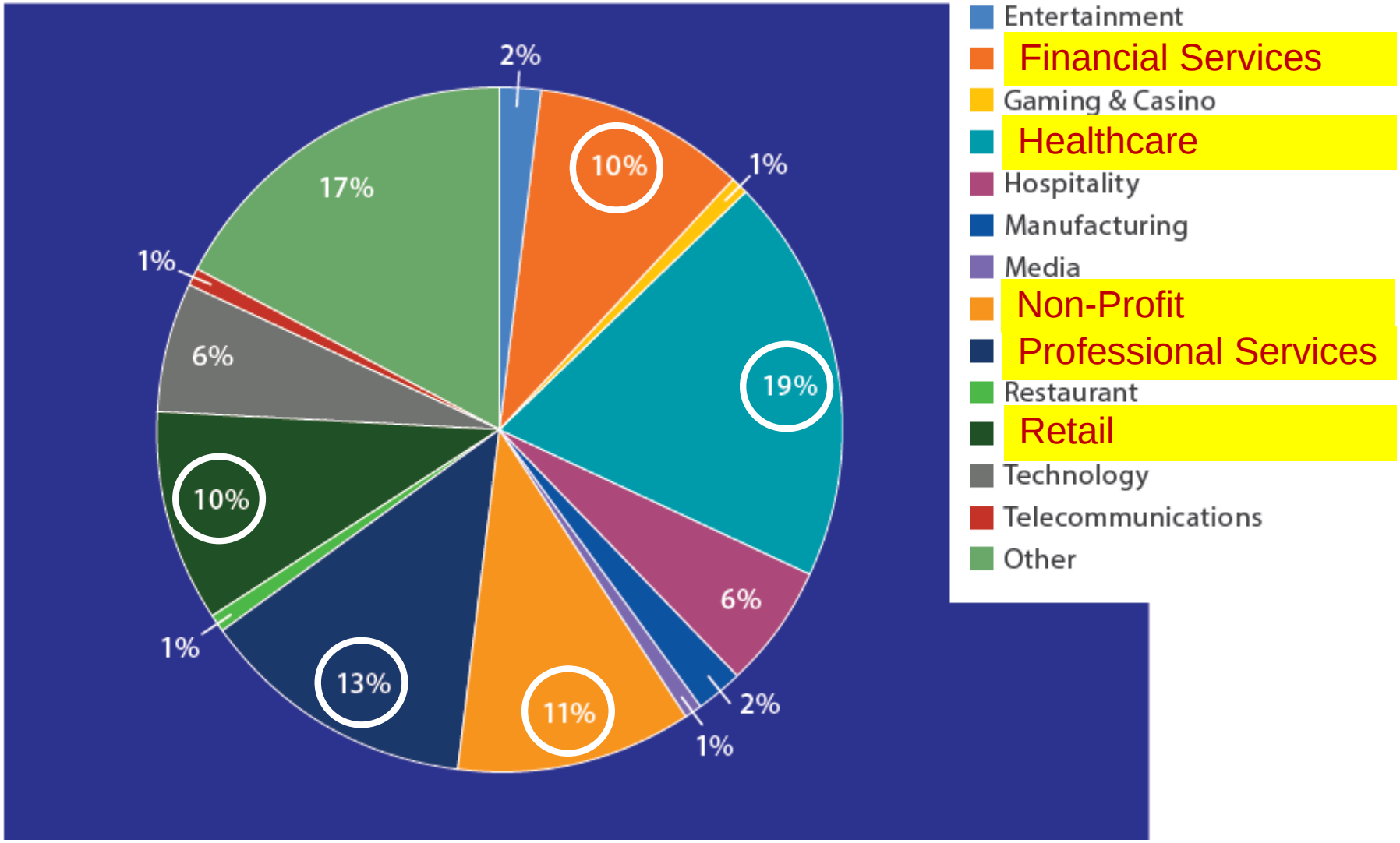


Who Are The Perpetrators?

Source: 2016/2017 Global Fraud & Risk Report – Kroll



What Are The Most Targeted Business Sectors?



Source: 2016 NetDiligence Cyber Claims Study

What Is The Threat Environment?

CRIMINAL

Hacking has become a mainstream activity for organized crime, targeting digital assets of an organization that can be acquired or sold on.

- Personal information
- Credit or debit card information
- Funds
- Intellectual property

HACKTIVIST

Hacktivists represent a formidable foe due to the technical capability of the individuals involved and can target organizations for a variety of reasons.

- Public support for a cause
- Direct impact of core activity
- Corporate or industry-wide scandal
- Top corporate brand target

TERRORIST OR STATE

The ability to create physical outcomes through the use of remote hacking of critical infrastructure represents an appealing option for terrorist groups.

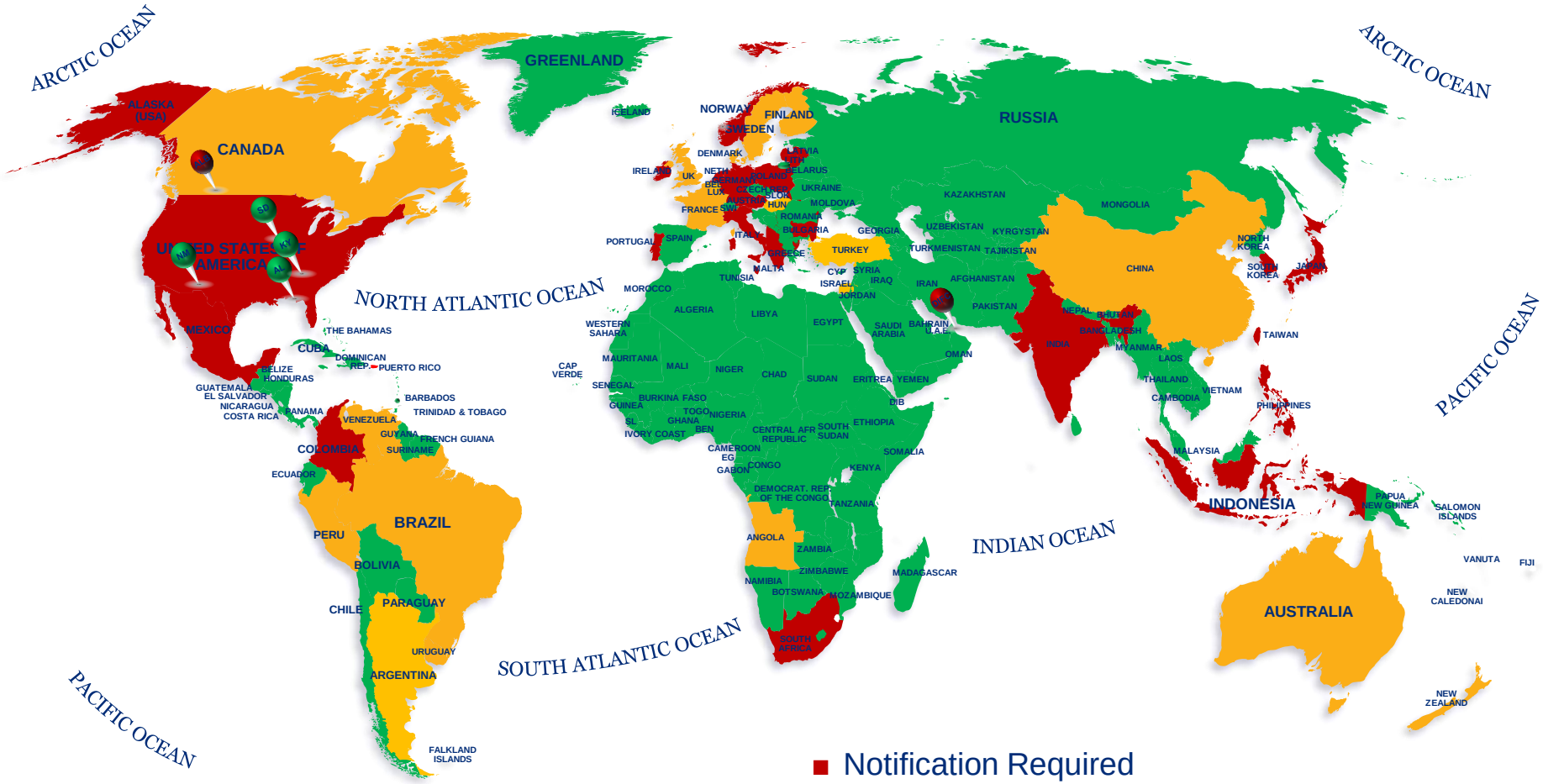
- Disruption to critical infrastructure
- Economic impact
- Loss of life
- Damage to property

MALICE

Where technical ability and motive combine, those who bear the organization ill are able to act maliciously by electronic means.

- Disgruntled employee or customer
- Proof of ability
- Untargeted malicious code
- Random selection

What Are The Breach Notification Requirements?



- Notification Required
- Notification Not Required but Certain Action Required or Recommended
- Notification Not Required

What Are The Breach Notification Requirements?

Capital market entities	Compliance by
Capital market entities identified by the SC	March 2017
Holders of Capital Markets Services Licence for: • Dealing in securities • Dealing in derivatives • Dealing in private retirement scheme • Advising on corporate finance; and/or • Fund management that are not identified to comply by March 2017	December 2017

All other capital market entities
• Capital Market Services Licence holders for:
  ○ Investment advice; and/or
  ○ Financial planning
• Bond pricing agency
• Credit rating agency
• Trustees
• Self-regulatory organisation
• Private Pension Administrator
• Registered market operators.
	December 2018

What Are The Breach Notification Requirements?

1. Contact information	
Contact details of the responsible person	
o Full name	
o Position	
o Office phone no.	
o Mobile no.	
o Email address	
Alternate contact person	
o Full name	
o Position	
o Office phone no.	
o Mobile no.	
o Email address	
Entity details	
o Entity name	
o Entity address	
o Type of entity (for example, financial institutions, participating organisation, exchange)	
o Contact no.	
o Email address	

What Are The Breach Notification Requirements?

2. Cyber incident or breach details	
o Date and time of incident or breach	1.45 am / 16 August 2016
o Details of cyber incident or breach - Method of the cyber attack - Duration of the cyber attack	(i) Distributed Denial of Service (DDoS). (ii) Approximately 3 hours.

What Are The Breach Notification Requirements?

3. Impact to systems, assets or information	
o Affected hardware	(i) 11 desktop computers at Processing Department and 3 computer servers. (ii) Back office processing of trading transactions terminated
o Affected software	(i) PO-Back End Process System
o Affected operating system	(i) Windows 10 (ii) RH Linux ver 100.100 (iii) Windows Server 10
o Impact to stakeholders	(i) Next day client's trading and payment information not updated on the entity's Back Office System. (ii) Possible theft of client's information
o Geographical location and IP address of attacker	(i) Possible IP address 31.12.257.257, Eastern Europe
4. Resolution of cyber incident or breach	
o What are the immediate remedial actions taken to minimise and mitigate risks from the cyber attack? o What is the current status or resolution of this incident or breach? ☐Resolved ☒Unresolved	(i) Internet connectivity was terminated. (ii) Entity's IT security and vendor was contacted to provide assistance to manage the situation and recommend remedial actions to be taken. (iii) Investigation on cyber breach is ongoing. More details expected within 24 hours.

Who is responsible under the PDPA 2013?

Section 133. Offences by body corporate

(1) If a body corporate commits an offence under this Act, any person who at the time of the commission of the offence was a director, chief executive officer, chief operating officer, manager, secretary or other similar officer of the body corporate or was purporting to act in any such capacity or was in any manner or to any extent responsible for the management of any of the affairs of the body corporate or was assisting in such management—

(a) may be charged severally or jointly in the same proceedings with the body corporate; and

(b) if the body corporate is found to have committed the offence, shall be deemed to have committed that offence unless, having regard to the nature of his functions in that capacity and to all circumstances, he proves—

(i) that the offence was committed without his knowledge, consent or connivance; and

(ii) that he had taken all reasonable precautions and exercised due diligence to prevent the commission of the offence.

Who is responsible under the PDPA 2013?

(2) If any person would be liable under this Act to any punishment or penalty for his act, omission, neglect or default, he shall be liable to the same punishment or penalty for every such act, omission, neglect or default of any employee or agent of his, or of the employee of the agent, if the act, omission, neglect or default was committed—

(a) by that person's employee in the course of his employment;

(b) by the agent when acting on behalf of that person; or

(c) by the employee of the agent in the course of his employment by the agent or otherwise on behalf of then agent acting on behalf of that person.

Marsh Solutions and Proven Approach

Marsh Solutions and Proven Approach
Cyber Risk Management Framework

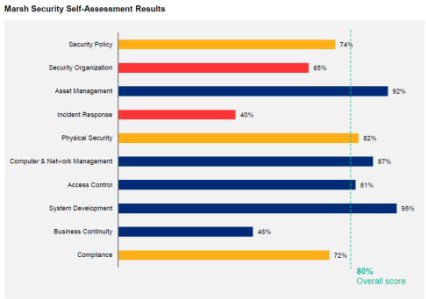
Marsh Risk Consulting (MRC) helps prospect assess, manage and respond to current or future cyber threats in an efficient and cost effective manner, using all available means to reduce the risk exposure.

- ✓ **Privacy and Information Security Assessment**
- ✓ **Non-Material Damage Business Interruption & Business Continuity**
- ✓ **Benchmarking & Quantification**
- ✓ **Risk Mapping & Coverage Gap Analysis**

Marsh Solutions and Proven Approach

Step 1: Privacy and Information Security Assessment

Assets	Threats	Control	Impact
What are my cyber assets?	**What are my threats?**	**What security controls do I have in place?**	**What is the impact of a breach?**
Begin by identifying, categorizing and ranking a client / prospect cyber-related assets. Assets form the motivations for threats against the organization.	Understand the cyber threats that correspond to the identified assets. Further, since cyberattacks are perpetrated by people – understanding how an organization looks to the world is paramount to understanding the likelihood of an attack.	How mature are the client / prospect defenses to protect against cyber-attacks? *Understand* processes, procedures, protocols, technical solutions and other measures that have been instituted. Compare those to the client / prospect peers and industry best practices to understand how ready they are for a cyber event.	Data breaches are one of the most common cyber risks faced by organizations today. A client / prospect should better understand the potential impact of a breach to the organization's assets, both qualitative and quantitatively, so they can prioritize their efforts to transfer or mitigate the risk of a breach.



Data Breach Event Total Costs

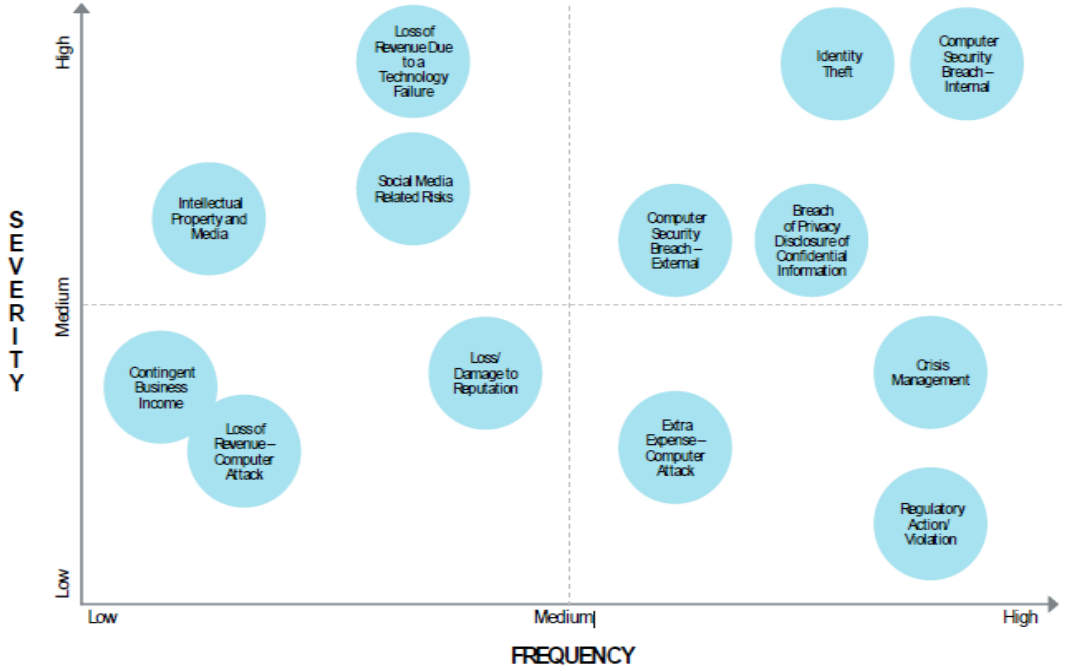
Event Type	Percentile	Number of Affected Records	Total Cost per Event
Mean	–	293,897	$2,034,491
1 in 2 Events	50%	5,176	$232,319
1 in 4 Events	75%	73,499	$495,939
1 in 5 Events	80%	142,851	$816,888
1 in 10 Events	90%	574,609	$3,746,131
1 in 20 Events	95%	1,570,302	$9,177,485
1 in 100 Events	99%	6,124,874	$38,061,069

Marsh Solutions and Proven Approach

Step 2: Risk Mapping

Taking what we learned from the privacy and information security assessment, we (along with our client / prospect) align risk management with the client / prospect objectives.

We will also prioritize the likelihood and severity of risks and identify any interrelationships among them.



Marsh Solutions and Proven Approach

Step 3: Benchmarking and Modeling

Privacy IDEAL Model (Identify Damages, Examine and Assess Limits)

- Developed by Marsh Global Analytics (MGA) to harmonize analytics offerings globally, aggregate data, and provide industry-leading analytics through cutting-edge technology.

Privacy IDEAL is built upon the following data sources

- Marsh proprietary Cyber Database
- Privacy Rights Clearinghouse Chronology of Data Breaches
- Advisen MSCAd Large Loss Database

Privacy IDEAL has two parts

- Frequency Model – predicts the likelihood of unauthorized disclosure.
- Severity Model – estimates the likely cost per breach.

Marsh Cyber Privacy Breach IDEAL Model

IDEAL is a dynamic decision support tool created by Marsh's cyber and actuarial experts to project a full range of outcomes to guide cyber insurance purchase decisions based on your company-specific inputs and historical data.

Modeling Assumptions for Sample Company

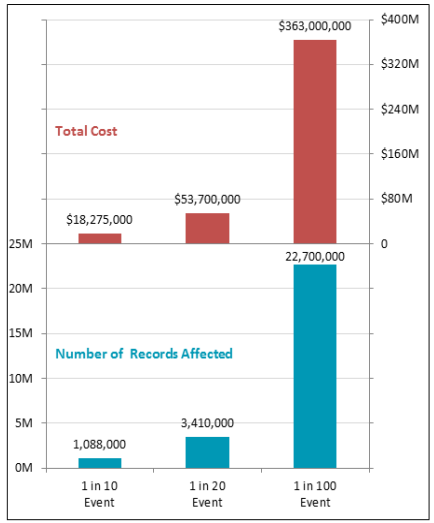
Industry:	Diversified Financial Services
Revenue:	$2,000,000,000
Security Level:	Average
Prior Breaches:	Zero
Cyence Threat Level:	High
Record Type	Total: 70,000,000
PCI:	8,750,525
PHI:	8,749,225
PII:	52,500,250

Frequency Projection

Based on the stated key assumptions, the probability that Sample Inc. will have at least one data breach event over the next 12 months is **6%**

Severity Projection

The graph and table below outline the potential severity cost estimate and associated affected records. Given a privacy exposure base of 70,000,000 records of blended PCI, PHI, and PII types, a 1 in 20 event affecting over 3.4M records could have a total cost over $53M. An extreme 1 in 100 data breach event affecting over 22.7M records could result in loss in excess of $360,000,000. We note that this modeling was based on estimated record counts and looks at different types of information differently.



Event Type	Total Cost
1 in 10 Event:	$18,275,000
1 in 20 Event:	$53,700,000
1 in 100 Event:	$363,000,000

Event Type	# of Records Affected
1 in 10 Event:	1,088,000
1 in 20 Event:	3,410,000
1 in 100 Event:	22,700,000

Sample Company Insurance Program vs. Severe 1 in 100 Event

	Program	% Covered
Total Cyber Limits:	$40,000,000	11%
Primary Retention:	$20,000,000	6%
Data Breach Costs Coverage Limits:	$25,000,000	7%
Data Breach Costs Retention:	$15,000,000	4%

MARSH

Marsh Solutions and Proven Approach

Step 4: Coverage Gap Analysis

Once we understand the client / profile risk profile, we will conduct a comprehensive gap analysis across all insurance product lines.

This will help determine what coverage is available to respond to claims and losses in the event of cyber attack, breach of privacy, or loss of confidential information.

Covered | Dependent upon specifics of claims and policy, may not be covered | Not covered

CATEGORY	LOSS ITEM	PROPERTY	TERRORISM	GENERAL LIABILITY	PROFESSIO INDEMNITY	FIDELITY (CRIME)	CYBER/PRIVACY POLICY
Assets	Destruction, corruption or theft of your electronic information assets/data due to a breach of computer or network security.						Information asset protection
Business interruption	Business interruption loss caused by a material interruption to your computer system due to a breach of computer or network security.						Network business interruption
	Business interruption loss caused by a material interruption to your computer system due to operational error of your staff.						Network business interruption
Privacy liability	Liability arising from the unauthorised release of personally identifiable information.						Privacy liability
	Costs incurred to notify affected individuals following the release of personally identifiable information where you are compelled to do so by law.						Privacy liability
	Defence costs incurred and penalties imposed (where insurable) in connection with a regulatory action brought as a result of the unauthorised release of personal information.						Privacy liability
	Payment Card Industry fines incurred as a result of the unauthorised release of credit/debit card information.						Privacy liability
Network liability	Liability arising from the failure of computer or network security to prevent a breach that damages a third party's data.						Network liability
	Liability arising from the negligent transmission of a computer virus caused by the failure of computer or network security to prevent a breach.						Network liability
	Liability arising from the prevention of authorised access to a computer system caused by the failure of computer or network security to prevent a breach.						Network liability
	Liability arising from the use by a hacker of your IT assets in a denial-of-service attack caused by the failure of computer or network security to prevent a breach.						Network liability
Electronic media liability	Liability arising from the content of your website(s) that is defamatory.						Electronic media liability
	Liability arising from the content of your website(s) that infringes another's intellectual property rights with exception of patent and trade secret.						Electronic media liability
	Liability arising from negligent publication or misrepresentation within the content of your website(s).						Electronic media liability
Extortion	Cost of a ransom paid as a result of a valid threat to release or destroy data assets including confidential commercial information or personally identifiable information.						Cyber extortion

Policies Terms and Conditions

Types of Insurance Policies

Policy Terms and Conditions
Coverage Parts

First Party Costs and Other Expenses

Reimburses an organization for the costs it may incur to respond to a breach

1) Business / Network Interruption
2) Event Management
3) Cyber Extortion

- Forensic Investigations
- Legal & Regulatory Advice Costs
- Notification Costs
- Account & Credit Monitoring Costs
- Data Asset Restoration
- Public Relations Costs

Third Party Liability and Defense Costs

Covers an organization's liability to third parties from its failure to keep data secure

1) Privacy and Data Breach
2) Failure of Network Security
3) Regulatory Investigations
4) Media Content Infringement, Libel, Slander, Defamation

Comprehensive Crime vs. Cyber

Comprehensive Crime Insuring Clauses
Covers Loss of Funds or Property

- Internal Crime (either acting alone or in collusion)
- External Crime
- Either for Financial Gain (for the perpetrator or someone else) or to cause a Loss to the Insured
- Contractual Penalties, Regulatory Penalties (insurable at law),
- Fees & Expenses
  - Legal Fees
  - Investigative Specialists Fees
  - Reconstitution costs
  - Reputation Recovery costs

Case Study – Global Investment Bank in US

Vulnerability of Data Leads to One of the Biggest Losses

- In 2014 – The hack began in June but it was not discovered until July when the hackers had already obtained the highest level of administrative privilege to dozens of the bank's computer servers.
- Over 83 million accounts were compromised – names, phone numbers, as well as mailing and email addresses.
- At the time of the breach, the bank had a cybersecurity team of 1,000+ and an annual budget of $250M.
- Total estimated cost of breach is a staggering **$12.8 billion** ($154 per record for data breach x 83M records)
- High profile, mega breaches tend to cost even more in reality. This number does not even factor in the loss of potential business.

Case Study – Malaysian Tech Company

CLAIMS EXAMPLE 1

We are an FSI company and we have an eCommerce trading platform, there is a DDOS attacked on our platform and our eCommerce service is interrupted by incident.

What policy do I need to protected the company against Loss of Business and Income and legal action by customers due to the incident and how to I make claim.

CLAIMS EXAMPLE 1

For the Loss of Business and Income - the Network Interruption Insurance (AIG) will be triggered. Time Excess (usually 8 – 12 hours) will apply before the policy pays.

The will pay ongoing fixed operational expenses plus loss net profit.

The policy will respond for the Increased Cost of Working if the insured needs to incur to mitigate or reduce the loss of income.

For the legal action by customers due to inability to access insured's network due to the cyberattack caused network outage – the Data Security Liability (AIG) will be triggered.

CLAIMS EXAMPLE 2

Ransomware has encrypted some of our critical business systems, business operation is disrupted and company and client data is lost and need to be rebuilt. We needs to engage with customers to rebuilt the data.

Can we claim against loss of income due to business interruption and data rebuilt costs ?

CLAIMS EXAMPLE 2

Yes for loss of income.

Yes for data rebuilt costs – Electronic Data (AIG) will be triggered.

Need to highlight this can trigger other extensions under the policy such as:

Data Liability (AIG)

Data Administrative Procedures (AIG)

Pro-active Forensic Services & Repair of Reputation cover (AIG)

CLAIMS EXAMPLE 3

In the event internal employee or hacker compromised our system and have stolen important data such as customer credits card data.

Can we claim on the costs related to customers claim against us on change of credit card costs, Forensic investigation cost.

CLAIMS EXAMPLE 3

The above shall trigger the Data Liability (AIG)

Also it can trigger:

Repair of Reputation cover (AIG)

Electronic Data (AIG)

Data Administrative Procedures (AIG)

Payment Card Industry Data Security Standards (PCIDDS) Cover (Allianz) – in the event the insured provides also platform for credit card payment by customer

CLAIMS EXAMPLE 4

We are a data centre provide hosting services to customer, there is an external attacks incidents which resulted denial of services to servers hosted by our clients. (e.g. DDOS or Ransomware for example)

Clients claiming damages against us due to the incidents, can we make a claim? what policy to purchase.

CLAIMS EXAMPLE 4

It w**ill trigger the <u>Data Security Liability</u> (AIG)**

MARSH