Data Breaches and How the Cyber Insurance Would Respond

As per Willis Towers Watson cyber claims analysis report (reported by clients from 2013 to December 2019 with total of number of claims nearly 1,200 claims from nearly 50 countries), data breaches are the most frequently reported losses and have the largest total amount of costs associated with them and malicious data breaches carried out by third-parties (as opposed to accidental data breaches by the company or malicious data breaches carried out by rogue employees) are the most frequently occurring and most expensive type of data breach loss.

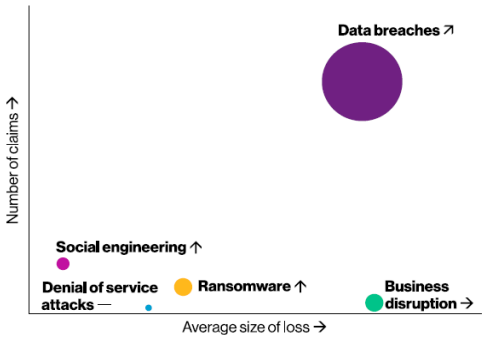
There is a huge variation in the size of data breach losses that we see, ranging from a single data subject to over a million impacted records. Whilst claims in this area are clearly divergent, the following can be discerned:

- The mean number of breached records per claim is over 693,000, whilst the median is much lower at 135.
- Nearly one in ten breaches involved more than 20,000 records.
- From our analysis, the direct event cost per breached record is $7.95.

Data Breach Loss Event

Overall, the chart shows that data breaches are the most frequently reported losses and have the largest total amount of costs associated with them.

Business disruption and ransomware events have a high average severity.



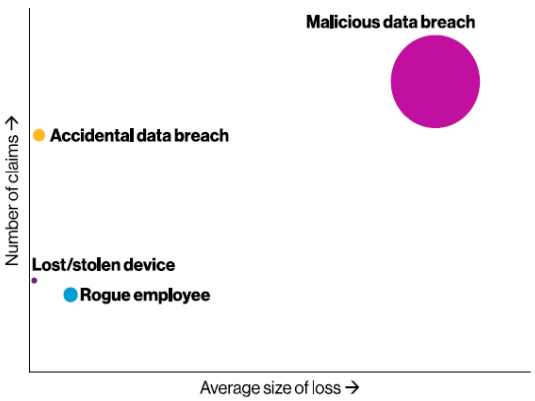
Willis Towers Watson

There has been a very noticeable increase in ransomware events in 2019. This low investment, low risk and high reward method of cybercrime has the added benefit to the criminals of the anonymity provided by receiving ransom payments in their chosen cryptocurrency.

Social engineering frauds are no longer just aiming to obtain funds via fraudulent transfer instructions. This method is now also being used to divert salary payments and fraudulently obtain tax data on employees. However, the most frequently notified social engineering event is still that of impersonation of a vendor/supplier.

Data breaches, in depth analysis

Data breaches come in many different forms, from sending e-mails with client details to unintended recipients, to hackers infiltrating systems to obtain payment card information. Below figure shows how these different types of losses rank in terms of frequency and severity.

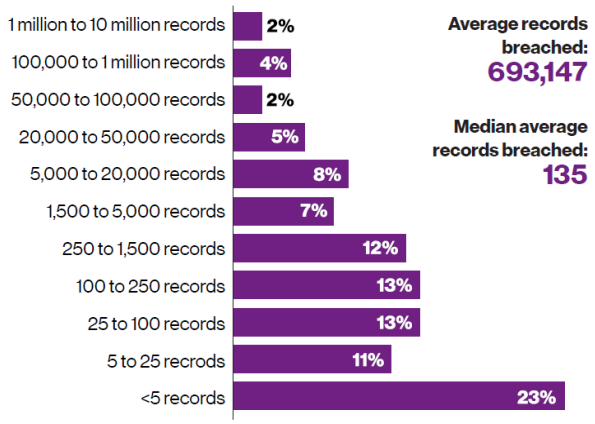


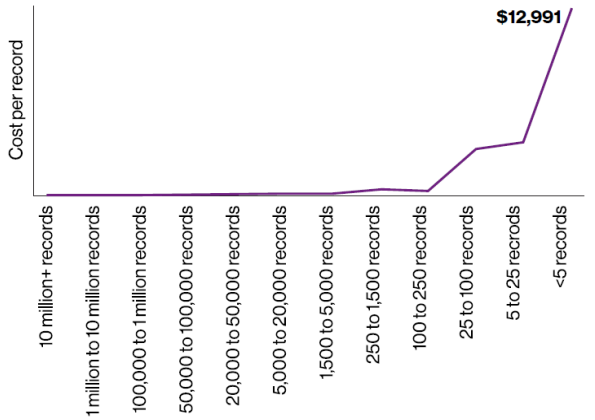
Data breaches – number of records

Below figure shows the number of distribution record breached for claims made under cyber policies. It shows that just 8% of breaches involved more than 50,000 records.

From our analysis, the direct event cost per breached record is $7.95. The figure also shows how the average cost per breached record varies according to the number of records breached. This shows when there are lower number of records impacted, the costs per record are relatively high.

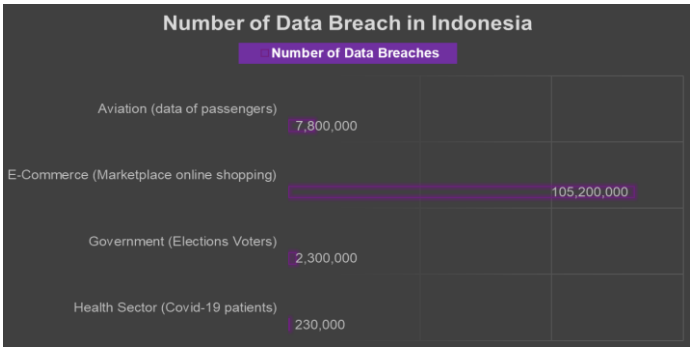
When the breach involves a higher number of records there are economies of scale (due to many crisis management and investigation costs being more fixed in nature) which reduce the costs per record significantly.





Data Breaches Incident in Indonesia

There were several incidents of data breaches in Indonesia which gave negative affect to stakeholders. As per CNN report, there were more than 5 massive incidents of data breaches occurred in Indonesia i.e. data breach of COVID-19 patients, data breach of election voters, some data breaches in E-commerce sectors. Those of data breach incident are mostly infiltrated by hackers. Most data stolen are consist of user ID, email, full name, date of birth, gender, mobile phone number including hashed password.



How Big is the Company's Financial Losses When Data Breach Occurs?

• When a data breach occurs, an investigation by an external IT Forensics Team will be required

When a data breach occurs, the company must immediately take action to understand the cause, scope and overall impact of the breach with the assistance of IT Forensic experts. For this reason, every company should have an "incident response plan" to help IT staff detect, respond to and recover from cyber security incidents, and involve external expertise when necessary. The complexity and the magnitude of potential losses must be minimized immediately by the forensic IT team.

Sufficient budgetary resources should be set aside for these events, particularly if the company wants to use a “Big Four” IT Forensic firm such as Mandiant or KPMG.

• Fulfillment of obligations towards law enforcement in Indonesia

When a data leak occurs, the Company is required to respond to any requests for information by the Regulator which will likely include providing information regarding what occurred, the scope of data loss, and steps taken so far to mitigate damage.

The results of investigations from the IT Forensics team can support the Company's legal team in complying with an investigation. Failure to comply with government regulation may result in verbal warnings, financial penalties, or the complete shutdown of business operations.

The Company will require the assistance of professional legal services to understand their immediate legal obligations when a data breach occurs. Errors in the fulfillment of reports and non-cooperation of the company in providing explanations and compliance with regulations may lead to fatal consequences such as the closure or suspension of the Company's operations.

• Third party claims such as clients, competitors, shareholders, etc.

Accidental or malicious data leaks may result in lawsuits from third parties who feel they have been negatively impacted by the event. Such third parties may allege that the company has failed to implement sufficient network security which resulted in the data breach (for example a hacked password will result in the illegal use of credit cards). This cost will usually be far greater than the initial incident response expenses as the company may need to defend themselves (with the help of a third party law firm) against such allegations in a court of law and pay any settlements if required. With class actions possible in Indonesia under several types of legislation - including Consumer Protection Law - companies can find themselves liable to reimburse a large group of people for the losses they have incurred.

• Damage to the Company's reputation

In some cases, companies will be unaware they have been impacted by a data breach until it is discovered on a public forum. Negative publications from the media can have a significant impact on the response from the public and may cause substantial damage to consumer trust and perceptions which may have taken years to build.

The role of the Company's Communications Team is to help reduce the negative response by making an official statement or apology that can restore the Company's reputation. In order to minimize negative news, collaboration with other professional and experienced Public Relations experts is needed to help restore the Company's reputation.

• Other costs

Companies will need to prepare a budget to provide notification of the data breach to their customers, set up a call center, and issue a letters of apology. Other costs such as compensation or gifts that aim to restore trust may be budgeted for if necessary.

If it is discovered in the course of the IT Forensics investigation that the company had weak IT security in place, improvements may be required in order to comply with regulation and prevent event reoccurring.

The above points outline the baseline costs associated with a cyber incident and while these may seem negligible, they can rapidly escalate. The worst-case scenario would be for the company to go bankrupt due to the diminished reputation and loss of trust from customers, or due to its operations being closed by the government either temporarily or permanently (because it cannot meet regulatory standards).

How can Cyber Insurance help?

Potential losses from cyber events can be measured and minimized using risk management strategies (Avoid, Reduce, Transfer, or Retain the risks). Cyber Insurance (i.e. Risk Transfer) is one tool that can help the Company manage a data breach or network outage which could cause a catastrophic financial loss too large for the company to retain themselves.

Cyber insurance can also provide organisations with peace of mind that they will be able to adequately respond to and recover from a cyber incident effectively and efficiently. Indeed, cyber insurance could provide the following benefits during data breach incident:

- A Breach Response Manager will be appointed immediately to understand the nature and details of the incident. This is commonly a law firm so we can establish legal privilege over the Claim from the very outset. The Breach Response Manager will, subject to the agreement of the Company and/or insurers, mobilise the members of the investigation team (including representatives of the Company) and begin the implementation of the Response Plan. Depending on the incident, and subject to the agreement of insurers & the Company, this may involve:
    - engaging IT forensics and other technical support to determine the cause of the cyber incident and to immediately commence preservation of all relevant operating logs;
    - determining what, if any, immediate actions need to be taken to mitigate the incident losses or extent of the losses;
    - engaging other third-party service providers including public relations firms, forensic accountants and credit monitoring services;
    - commencing the process of notifying the regulator and individual customers of the policyholder, as appropriate;
    - determining if any public announcement is to be made;
    - responding to enquiries of the policyholder;
    - considering the reports on the cause of the incident and findings of the IT forensics and advise whether any remedial services are required; and
    - assist the Company to resume business as usual.

All the above costs will be fully covered by the Insurance Company (subject to policy terms and conditions).

How to ensure effective Cyber Insurance protection?

Prior to making a purchase of cyber insurance, companies need to have an in-depth analysis of business risks and exposure. Loss due to cyber risks can be measured qualitatively and quantitatively and a step-by-step approach can be taken to ensure effective risk transfer.

1. Diagnose organizational capabilities regarding cyber security using the standard cybersecurity frameworks issued by NIST (National Institute of Standards and Technology) or ISO standards.

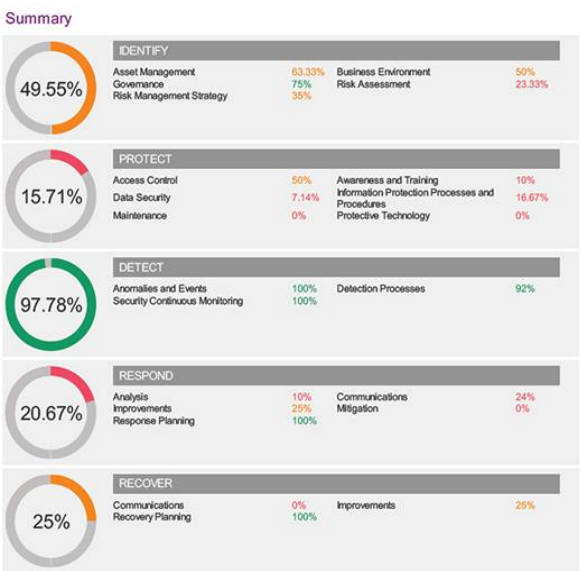


Figure 6 : Sample of Perils Diagnostic Assessment as per NIST

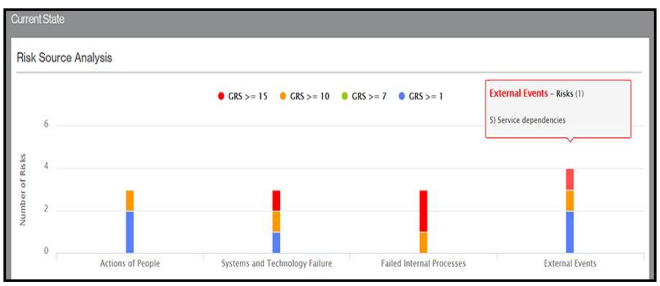
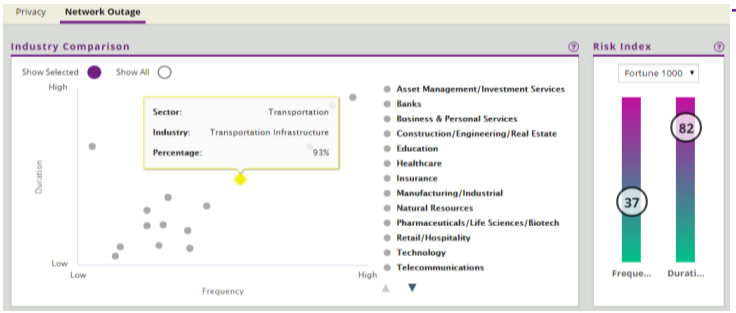


Figure 7 : Risk Source Analysis as per NIST

2. Evaluate the financial impact of a data breach of network outage on the company, looking at frequency and severity.



- The most likely cost associated with 100k, 1M, and 10M record breaches for PCI data. See cost calculator online for more detail.

	100K Records	1M Records	10M Records
Breach Expenses	393,260	1,774,440	3,335,820
Breach Response Costs	1,011,240	7,261,000	46,287,020
Regulatory Fines & Defense	106,000	1,060,000	5,300,000
PCI Fines/Penalties	20,076	501,894	1,003,788
Civil Liability	1,195,680	9,889,800	74,814,800
Total Cost	2,726,256	20,487,134	130,741,428
Cost Per Record	27.3	20.5	13.1

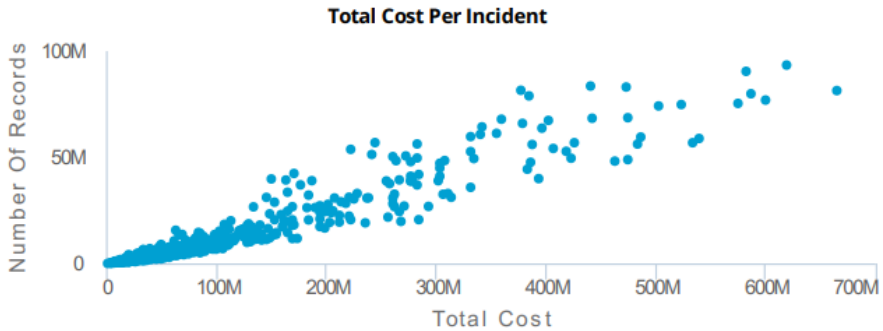


Figure 8 : sample of Cyber risk quantification modelling

3. Conduct a deeper analysis of Cyber Risk by creating cyber risk scenarios in the Company such as how large the impact and likelihood will occur. At this stage input is needed from Operations, IT, Finance, Legal, Compliance, Risk Management, etc.

Willis Towers Watson

Cyber Risk Assessment and Quantification
Industrial Control Systems and Enterprise Information Technology

			Property damage repair/replacement costs				System and software repair/upgrade costs				Liabilities to third parties - dama	
			Amount		Probability		Amount		Probability		Amount	
SCENARIO	SCENARIO & SUB-SCENARIO DESCRIPTION	LIKELIHOOD	Low	High		Notes	Low	High		Notes	Low	High
			1,005,000	257,350,000			0	5,000,000			0	250,000,000
1	**Abuse of authorized computer/network access and/or violation of IT security mechanisms**											
Most likely	Misuse/stealing of sensitive data of organisation or its employees, by employee (e.g. including publishing content in electronic or print media, or on social media platforms)	1 to 10 losses in a year	100,000	1,000,000	10%	Minimal impact. Replacement costs	50,000	500,000	0%	No change in systems of process	0	500,000
Mid Range	Business Unit 1 - ICS software modified/infected or configuration settings modified, by third party and employees	1 loss in 5-10 years	50,000	40,000,000	30%	Possible damage to 3	25,000	1,000,000	0%	Changes/upgrades in systems	0	2,000,000
Worst Case	Business Unit 2 - ICS software modified/infected or configuration settings modified, by third party and employees	1 loss in 10-25 years	50,000	70,000,000	20%	Based on financial elements ranges	25,000	1,000,000	0%	and process are integrated	0	5,000,000
2	**Cyber espionage (Competitors, Nation States, etc)**											
Most likely	Stolen portable device (e.g. USB drive, laptop) or back up media (e.g. including tape drives, cloud systems)	1 to 10 losses in a year	100,000	1,000,000	100%	Replacement costs, equipment	2,000	50,000	20%		0	50,000
Mid Range	Data breaches (e.g. to steal intellectual property or financially or legally sensitive data)	1 loss in 1-5 years	50,000	10,000,000	15%		0	0	0%		0	0
Worst Case	Identity theft with the purpose of financial fraud or operational disruptions	1 loss in 25-100 years	50,000	25,000,000	40%	Possible damage to 3	0	0	0%		0	0
3	**Crimeware & Targeted Attacks**											
Most likely	Enterprise IT Ransomware (e.g. demand to terminate attack on system or data breach) and Malware	1 to 2 losses in a year	5,000	100,000	30%	Equipment is recoded/ref	30,000	400,000	20%	Changes/upgrades in systems and	30,000	1,000,000

In order to have proper and optimum risk transfer with having cyber insurance, a company can use insurance brokerage services that can combine all the above elements so that the company can choose the optimal insurance program and carry out effective risk transfers.

Conclusion

Cyber risk is now become emerging risk in Indonesia that need to be placed by stakeholders as one of top priority risks that would significantly affect their businesses. One of cyber risks that may significantly affect the business is Data Breach. It has been proven; such risk has been ruining business of many companies in the world as well as in Indonesia.

Every company would need to consider their current risk management approach and strategy for cyber risks including protecting their internal and customers' data because data have a high value and it should be protected. Having cyber insurance would be beneficial for companies even though they already have strong cyber security team or how cyber savvy they are as indeed still would have many gaps and also human errors that would lead to data breach incidents. For sure, those risks that need to be transferred to insurance company.

However, prior to making a purchase of cyber insurance, companies need to have an in-depth analysis of business risks and exposures. Companies should look how much cost versus benefit to have insurance by measuring their cyber risks qualitatively and quantitatively in order to have ensured effective risk transfer. You can contact your insurance consultant or us to discuss about your data breach exposures.

Author: Damy Nugraha
Head of FINEX
Willis Towers Watson Indonesia

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

willistowerswatson.com

Willis Towers Watson