

No organization is immune to cyber risk

I am planning to put cyber risk as one of my risk management initiative for this year, however my CEO think that it is not necessary because our organization is non high tech. Is there any reference on which industries that need to consider cyber risk in its risk assessment?

Hendra, Cikarang

For some, the terminology of Cyber Risk is unthinkable and unlikely to occur, especially when you work at an organization with simple IT environment.

The common perception is that cybercriminal only interested in companies in certain industries such as e-commerce, bank, telecommunication, unfortunately the fact say otherwise. The recent Panama Papers scandal has proven that.

Data Theft

Mossack Fonseca is not a high-tech company; it is a law firm and corporate service provider. What has happened was someone with unauthorized access steals 2.6 terabyte data from their database. The data consist of 11.5 million files that contain client's confidential data from 40 years ago that connect more than 214,000 offshore companies to people in more than 200 countries.

We do not know whether the "attacker" ask for some money from Mossack Fonseca or from the people on the list before they "share" the file to ICIJ (The International Consortium of Investigative Journalists).

However one thing for sure is that the Panama Papers has harm Mossack Fonseca reputation as well as the people in the list.

Ransomware

Let me give you another example of cyber risk that is not targeting complex IT or a high-tech company, there is a phenomenon of ransomware attacking healthcare industry and individual.

Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid.

Once your computer is infected by ransomware, you cannot access your document important files, photos or even music in your computer before you pay some money to the "attacker".

Last month, attackers took computers belonging to the Hollywood Presbyterian Medical Center in Los Angeles hostage using a piece of ransomware called Locky. Computers were offline for more than a week until officials caved to the extortionists' and paid the equivalent of \$17,000 in Bitcoin.

How about in Indonesia?

A couple months ago, one of graphic designer in Indonesia was also being a victim of ransomware.

All Sectors are Prone to Cyber-Attacks

From some of the samples provided, we can see that no single organization is immune from cyber risk.

The need for a cyber risk assessment is not determined by the complexity of IT used in an organization, and the risk is not exclusive only for certain industries.

Every organization needs to have a cyber risk assessment. All sectors are prone to cyber-attacks, and those attacks could be of any nature and they have the potential to damage not only the records, but also the reputation of your organization.

The minimum is to identify what impact does the cyber world brings to your organization.

From there, you can design a mitigation plan and action to reduce the likelihood of its happening as well as to reduce the exposure of it when it happens.

KEY POINTS

- Data and information are important and valuable asset in this digital age.
- Need for a cyber risk assessment is not determined by the complexity of IT within an organization.
- Cyber risk assessment is needed to identify exposures and to design the mitigation plan.



Ponda Hidajat

**Partner
Governance Risk Control**

ponda.hidajat@rsmindonesia.id

THE POWER OF BEING UNDERSTOOD

Wake Up Call is a consultancy column designated to discuss questions related to audit, accounting, tax, corporate finance, business services, governance, risk management, internal audit, and internal control. RSM Indonesia is a member of the RSM network and trades as RSM. RSM is the trading name used by the members of the RSM network, the 6th largest network global audit, tax and consulting services. RSM network has representative in more than 120 countries, and a combined total of 38,000 staff including 3,000 partners in 760 offices. Questions can be submitted to wakeupcall@rsmindonesia.id.