MAKLER S.A.
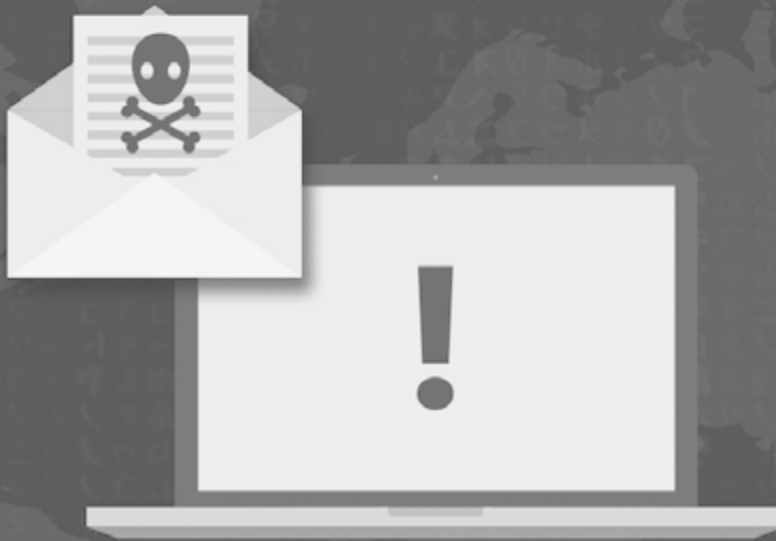
ASESORES EN SEGUROS

Great **solutions**,
better *results*.

CYBER RISKS

CYBER RISKS

Cyber attacks are not something that "might happen to us", these occur at all times, every day, and in a matter of seconds can become a devastating problem.

What is a Cyber Risk?

A Cyber Risk is any exposure to a financial or operational loss or damage to an organization's reputation as a result of it's flaws in its information technology systems, the processes that support them, or the use of information by third parties who could have access thereto.

The origins of these exposures range from cyber attacks; system viruses and ill intened e-mails, to human errors; employees seeking to obatin benefits in a fraudulent manner; or the inadequate use of information by providers, amongst others.

Cyber risks are not always related to technological threats or cyber criminals, nor is their goal always to obtain a financial or economic benefit. Some attacks are driven, for example, by an act of vengeance; for firing an employee; the emotion arising from causing damage; or simply the challenge of executing a successful attack.

How can an organization be affected by a cyber attack?

» Loss of revenue/money
» Being used as an access route to greater objectives through its role or its products and services in a supply chain.
» Loss of critical information necessary to administrate the business.
» Suffering reputational damage that can negatively affect a customer's opinion.
» Loss of income as a result of interruption of activity.
» Receiving sanctions from government control entities as a result of the wrongful use of information.
» Being sued or receiving claims from people who are affected by the wrongful use of confidential information.

58%
of attacked victims are small and medium sized organizations.

92.4%
of these attacks are received via e-mails.

60%
of small and medium organizations throughout the world indicate more severe and sophisticated attacks.

1 of every 5
small and medium organizations are victims of cyber crimes.

50%
of major corporations have been attacked over the last year.

70%
of these have kept silent.

Despite the fact that people are not as concerned as they should be given the silence from small and mediaum organizations, every day **15 million** cyber attacks are generated throughout the world.

Who do we cover?

The insured organization.

Any person that is, has been, or becomes a member of an organization's board; General Manager; or partner.

Any employee of an organization (including the Compliance Officer; the Data Protection Officer; and the Director of Legal Affairs).

Coverage

Damage to the insured party
- » Recovery of digital information.
- » Interruption of business activities.
- » Cyber extorsion.
- » Fraudulent banking transactions.

Damage to third parties
- » Liability arising from leakage of confidential and or personal information.
- » Liability arising from the use of malicious software or spreading of system viruses.
- » Publishing in digital media.
- » Defense and litigation expenses.

Crisis Management
- » Expenses incurred to protect reputation.
- » Forensic expenses.
- » Defense expenses – Administrative Authorities.
- » Expenses lacking previous authorization.

We **proposed** it to ourselves
and we **made it.**
Our first**39**years!

makler s.a.
ASESORES EN SEGUROS

www.**maklerseguros**.com.ar