CyberSolid

Gold Standard for your Cyber Risks

GrECo,
matter of trust.

Cybercrime. One of the top corporate risks worldwide.

The danger of cybercrime continues to grow and has become a global threat to all businesses, regardless of national borders, size or industry. IT security has developed to a priority for companies looking to protect their data and systems. But even with cyber security measures in place, breaches do happen and can prove incredibly costly. That's why cyber insurance is so important. It protects you against the consequences of cyber-events by providing financial compensation and crisis management when things go wrong.

Cyber threats for your business

In today's digitalized world, new risks emerge every day. Connecting to the internet opens up the possibility of a hacker targeting your organization. Not only large corporate organizations are at risk. Small and medium sized businesses are also vulnerable to cyber-events that result in a range of business impacts including ransom demands, business interruption, corrupted data and compromised personal information.

The following cyber threats can be significant, involving loss of data, blackmailing and the cost of rebuilding computer systems:

Ransomware
Ransomware is a type of malware designed to deny access to a computer system or data by encrypting the information and holding it "hostage" until the ransom is paid.

Phishing
Phishing is a form of internet fraud where an attacker attempts to obtain sensitive information by pretending to be someone of familiarity through the use of electronic communication such as email or telephone.

Data breaches
Data breach is an action where sensitive information is transferred from a computer or data center to the outside world either intentionally or accidentally. This type of security incident can be damaging, costly and takes time to repair.

Hacking
Criminally breaking into computer systems to damage or steal data is very profitable for hackers. Their motivation can be a number of reasons, like profit, protest, information gathering or challenge.

Insider Threat
The losses from insider cyber threats can be significant often because the insider knows exactly where to look to obtain access and how to overcome existing security measures.

Claims examples.

Cyber-events and data breaches are occurring more frequently and at a larger cost. There are many different ways to experience a data breach or business interruption event.

An employee of a law firm accidently downloaded a destructive computer virus onto the company's network, resulting in data loss and transmission of the virus to a client's computer network. The client sued the company, contending it should have prevented transmission of the virus.

Damages and settlement: 750,000 EUR.

A retail chain was subject to a sophisticated hack which led to a data compromise of several thousands of its current and former customers. The attackers gained unauthorized access of the IT system and had obtained personal information of the customers of the company.

Damages and settlement: 220,000 EUR.

An employee at an engineering firm found a way through his company's network security defenses and gained access to a customer's trade secret. The employee sold the trade secret to a competitor. The customer sued the engineering firm for the failure to protect the trade secret.

Damages and settlement: 450,000 EUR.

A construction company was a victim of a virus attack, infecting multiple PCs and servers. The company was not able to operate for weeks. The scope of the infection revealed it was less to replace computers and the server instead of deleting systems, reformatting the drives and rebuilding them.

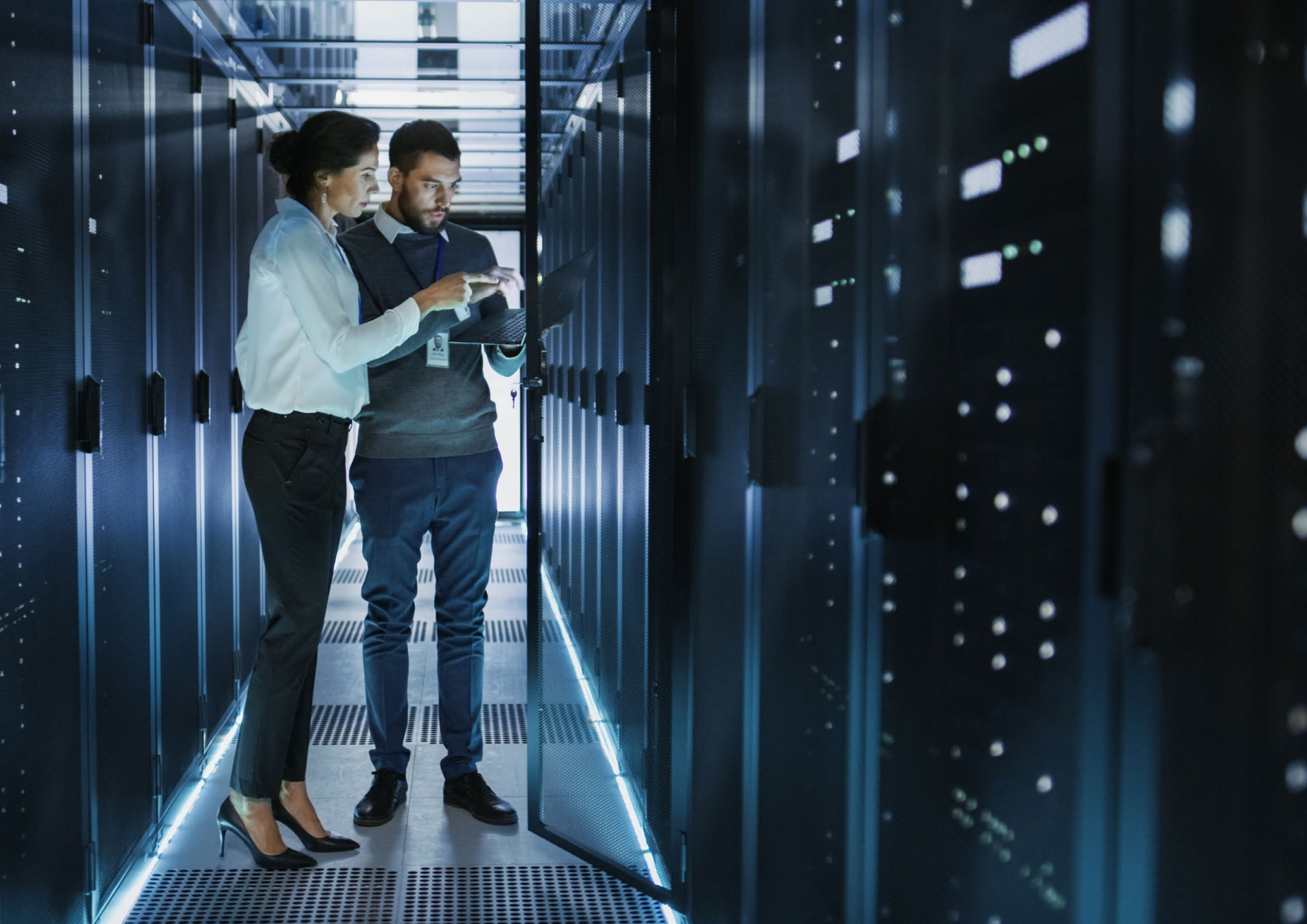
Damages and settlement: 1,000,000 EUR.

The computer system of a healthcare organization, which held medical information on their patients, was compromised by a ransomware attack. As it turned out that it was not possible to access the patient's medical data, they were unable to operate.

Damages and settlement: 124,000 EUR.

A hotel was hacked by someone who stole the identity and bank account details of its employees and guests. The information was sold to a website which uses the information to create false identities.

The damages and settlement resulting from violation of the GDPR and the lawsuits exceeded 900,000 EUR.



CyberSolid. The comprehensive protection for your company.

GrECo offers cyber insurance that is specifically designed to cover all threats of today's digitalized world.

CyberSolid completes your cyber security measures by providing holistic coverage:

- Data Breach: disclosure or loss or theft of personal data or confidential information
- Cyber-attack: attack designed to disrupt access to or the operation of a computer system
- Privacy and Security liability: claims and investigations against you
- Operational error: any error in the operation or maintenance of your data or computer system

If any of the above is triggered CyberSolid covers the following:

Your own losses:

Breach costs

Data recovery costs

Business income loss

Cyber ransom losses

Reputation protection

Claims and investigations against you:

Privacy liability

Network security liability

Privacy investigation costs

Privacy forensic costs

Online liability

Highlights

- Response with a 24/7 hotline to a proven crisis manager.
- Manages data breaches with forensic investigations, legal advice and notifies customers or regulators.
- Compensates for loss of income as a result of a breach.
- Protects you for any GDPR non-compliance claims.
- Covers also breach by suppliers and operational error.

Cyber insurance self-assessment

Whether your data is held for ransom, your clients' financial information is stolen, or your servers fell victim to an attack, cyber risks are everywhere. And in a world where data exists in digital form, you can't afford not to protect it.

Your traditional lines like property insurance and liability insurance usually don't cover your cyber exposure.

We recommend to ask the following questions:

Do you store (other) business-critical information?

Losing access to corporate information (i.e. designs and plans, client contracts, or stock levels, etc.) for an extended period of time can cripple your ability to operate.

☐ yes

Do any of your employees work remotely?

Logging in from other networks can pose a risk, and remote networks aren't immune to attack. Employees may also lose devices.

☐ yes

Do you collect or store personal data?

You would have to notify if sensitive data is lost or stolen (like names, email addresses, billing addresses, credit card numbers, phone numbers, or health information…)

☐ yes

Can your business operate without access to your computer systems or data?

We have seen clients who are down for 2-3 day in the least, up to weeks or months at worst.

☐ yes

Is your business relying on your good reputation?

Companies that suffer a cyber-attack can find the biggest damage is to their reputation.

☐ yes

Are you afraid that you or your employees will never make a mistake?

The vast majority of cyber incidents involve some kind of human error of oversight.

☐ yes

If the answer to these questions is predominantly yes, we recommend a risk dialogue with our cyber specialists. GrECo has over 10 years of experience in insuring cyber risks and has proven this experience in many claims.

Contact

Anita Molitor
Cyber Specialist
T +43 5 04 04 374 | M +43 664 962 40 08
a.molitor@greco.services

GrECo Specialty GmbH
Insurance Brokers and Insurance Consultants
Elmargasse 2-4 | 1190 Vienna
www.greco.services

GrECo,
matter of trust.