Blog

Cyber Resilience – A vital concept in today's world

Sergio P. Ermotti
Chairman of the Board of Directors, non-executive and independent

12 Apr 2022

Follow Share

Cyber risks have been an important topic for quite some time. But the COVID-19 pandemic and Russia's invasion of Ukraine have made them even more prominent. Working virtually from the home office and the use of the internet for a much broader range of services have increased exposure and our dependency on technology. In today's world, whenever there are conflicts, we expect cyber operations to accompany them – from classic espionage to disrupting critical infrastructures and military operations, psychological warfare, and misinformation.

Already the sharp increase in cyberattacks in recent years has brought to light two facts that many people were previously unaware of or at least strongly underestimated: First, the business world is highly interconnected. And second, the digitalization of business processes is already so advanced that many companies cannot function when data or their systems are not available.

One of the most important principles in cyber is that there is no 100% security

As cyber risks, or more generally digital risks, become top business risks, cyber resilience becomes vital for all types of businesses. If you honor that principle, you understand that you not only have to protect yourself against cyber risks, but also be prepared for an event to happen.

- Cyber resilience is an organization's ability to deliver a sufficient level of business services despite adverse cyber events.
- This capacity to deliver must be comprehensive, and also include the supply chain.
- To maintain cyber resilience, the organization must have a formal information security program, a dedicated team and a governance system that are integrated with the risk, crisis, business continuity, and education programs.

I strongly believe that insurance has an important role to play in the cyber resilience of organizations. There is, however, another important principle: Insurance can be part of the solution, it is not the sole solution. The contribution insurance can make is to help mitigate the financial impact from these risks, to deliver concrete cyber risk management service and to help increase overall cyber maturity, all this subject to a proper level of cyber resilience as mentioned above.

What is covered by cyber insurance?

Cyber insurance covers risks arising from issues with confidentiality, integrity or availability of data. One important coverage is liability for data privacy breaches. Companies that store or process personally identifiable information are required to keep that information confidential and secure. If the data is stolen and made public, the company is liable. In this case, cyber insurance would in principle cover possible payments to the affected individuals, legal and litigation costs, notification costs and the establishment of call centres if necessary, as well as credit monitoring costs in some jurisdictions.

Availability of data is key to any digitized process in the economy. If data is not available - for example in the case of a ransomware attack where attackers encrypt the data and only release the key after a ransom is paid - there may be a prolonged business interruption. Cyber insurance can cover the lost business during this interruption and helps the affected company resume normal operations as quickly as possible.

Cyber insurance goes beyond pure risk transfer

Many cyber insurance products include services to help the insured manage a cyber event. These may be incident response services, often provided by a specialized company on behalf of the insurer. If an insured company is hit by a cyber event, they can call a hotline and receive direct help, like IT forensics services or crisis management support. Other services might be of a more preventative character, for example employee trainings, that can be rolled out to the organization.

There are conditions for insurance

A very different but no less important factor are the base requirements that insurers ask of their insureds. These requirements may be formulated during the risk assessment process before the insurance policy is issued, often in the form of check-lists, questionnaires or risk dialogues. Or they may be included in the policy itself as obligations that the insured must fulfil during the term of the policy.

In the past, many people have pointed to this concept and to insurers to increase the overall cyber maturity by generating "security standards" for the market. However, with a very soft insurance market and ample risk capacity available, this mechanism did not work for some time. Today, however, we are in a different world, and insurers are asking clients to secure better protection and boost their preparedness before insuring a risk.

Thus, cyber insurance goes beyond pure risk transfer and contributes directly to improved organizational risk management and increased cyber resilience.

There are limits to coverage

When talking about cyber risks one often has this picture of a hooded hacker in one's mind, sitting in a darkened room and hacking into a company's network. While malicious attacks are certainly an important risk vector, cyber risks also result from human or system errors. There are numerous examples where companies or health-care providers accidentally published customer or patient data by mistake and thus created a data privacy event.

An exception to standard coverage is war. War is typically excluded in property and the same is true for cyber insurance. The reason for this is that the damage potential in the event of war is so high that it exceeds the financial might of the private insurance industry and insurance policies would simply be too expensive if this risk was properly priced in.

However cyber risks develop in the future, insurance can help manage those risks and contribute to organizational, but also on a larger scale, to societal cyber resilience.

** Based on a speech Sergio Ermotti has given at the American Swiss Foundation, 8. April 2022*

cyber | driving digital insurance solutions | infrastructure | technology | reinsurance | insurance | digitalisation | big data

YOUR EXPERT

Sergio P. Ermotti

Chairman of the Board of Directors, non-executive and independent

View profile

FIND FURTHER COVID-19 CONTENT

Share Price

CHF 00.0 – 0.0%

, CET

Newsletters

Subscribe

Contact us

Contact