WHY CYBER INSURANCE IS IMPORTANT

The loss, compromise or theft of electronic data can have a negative impact on a business, including the loss of customers and revenue.

Businesses may be liable for damages stemming from the theft of third-party data. Cyber liability coverage is important to protect businesses against the risk of
cyber events, including those associated with terrorism. Cyber-risk coverage can assist in the timely remediation of cyberattacks and incidents.

In 2011, Sony's PlayStation Network was breached by hackers, exposing personally identifiable information (PII) of 77 million PlayStation user accounts. The breach prevented users of PlayStation consoles from accessing the service, an outage that lasted for 23 days.

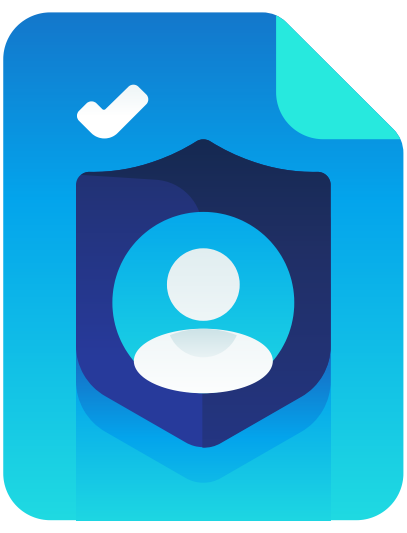
Sony incurred over $171 million in costs related to the breach. Portions of this cost could have been covered by a **cyber insurance policy**, but Sony did not have one in place. A court case ruled that Sony's insurance policy covered damage to physical property only, leaving Sony to incur the full amount of costs related to cyber damages.

HOW CYBER INSURANCE WORKS

Cyber insurance policies are sold by many of the same suppliers that provide related business insurance, such as E&O insurance, business liability insurance and commercial property insurance.

Most policies include first-party coverage, which applies to losses that directly impact a company, and third-party coverage, which applies to losses suffered by others from a cyber event or incident, based on their business relationship with that company.

Cyber insurance policies help cover the financial losses that result from cyber events and incidents. In addition, cyber-risk coverage helps with the costs associated with remediation, including payment for the legal assistance, investigators, crisis communicators, and customer credits or refunds.



WHO NEEDS CYBER INSURANCE?

Businesses that create, store and manage electronic data online, such as customer contacts, customer sales, PII and credit card numbers, can benefit from cyber insurance. In addition, ecommerce businesses can benefit from cyber insurance, since downtime related to cyber incidents can cause a loss in sales and customers.

Similarly, any business that stores customer information on a website can benefit from the liability coverage that cyber insurance policies provide.

WHAT IS COVERED AND NOT COVERED BY CYBER INSURANCE?

Depending on the price and type of policy, the customer can expect to be covered for extra
expenditures resulting from the physical destruction or theft of information technology (IT) assets.
Such expenditures typically include costs associated with the following:

- meeting extortion demands from a ransomware attack;
- notifying customers when a security breach has occurred;
- paying legal fees levied as a result of privacy violations;
- hiring computer forensics experts to recover compromised data;
- restoring identities of customers whose PII was compromised.
- recovering data that has been altered or stolen; and
- repairing or replacing damaged or compromised computer systems.

Traditional insurance policies typically exclude cyber-risks, and this has led to the growth of cybersecurity insurance as a separate, stand-alone type of coverage. Potential customers include any company that accepts digital payments or stores PII about customers, including medical and financial information.

Some cyber insurance policies cover the cost of providing credit monitoring services for customers affected by a data breach. In September 2017, Equifax, a consumer credit reporting agency, suffered a data breach that exposed the personal information of 147 million people. In 2019, Equifax reached a settlement with the U.S. Federal Trade Commission (FTC).

As part of the settlement, Equifax agreed to spend $425 million to provide free credit reporting, cash payments -- e.g., for those already enrolled with a credit monitoring service -- reimbursement for time or money spent on recovering from identity theft and free identity restoration services. A cyber insurance policy could have paid for part of the $425 million cost of Equifax's settlement, assuming the circumstances of its data breach were covered by such a policy.

Many entry-level cybersecurity insurance policies only cover first-party losses, but some insurers are beginning to offer policies that cover third-party liability losses as well.

Many cybersecurity policies exclude preventable security issues caused by humans, such as poor configuration management or the careless mishandling of digital assets. Other issues excluded by cybersecurity policies include the following:

- pre-existing or prior breaches or cyber events, such as incidents that occurred before the policy was purchased;
- cyber events initiated and caused by employees or insiders;
- infrastructure failures not caused by a purposeful cyber attack;
- failure to correct a known vulnerability, such as a company that knows that a vulnerability exists,
- fails to address it and is then compromised from that vulnerability; and
- the cost to improve technology systems, including security hardening in systems or applications.