iStore Business – infoSec Cyber Security Warranty

Option 1 - Included	Limit
Data Breach	R500 000
IoT Event	R125 000
Business Email Compromise	R250 000
Cyber Extortion	R125 000
Option 2 - +R450pm	**Limit**
Data Breach	R500 000
IoT	R250 000
Business Email Compromise	R250 000
Cyber Extortion	R250 000
Option 3 - + R600pm	**Limit**
Data Breach	R1 000 000
IoT	R250 000
Business Email Compromise	R250 000
Cyber Extortion	R500 000

Contact us

infosec@istorebusiness.co.za

https://www.istore.co.za/business-info-security

iStore Business

Core Peripherals (Pty) Ltd trading as iStore Business
Reg No: 1996/010298/07 | Vat No: 4190160756

DATA BREACH

A data breach is an incident where sensitive, protected, or confidential data is accessed, disclosed, or stolen by unauthorized parties. This can include personal data like names, financial records, or company proprietary information. Data breaches often occur due to weak security controls, vulnerabilities, or malicious attacks, and can lead to reputational damage, legal liabilities, and significant financial losses for the affected organization.

The Warranty includes costs to respond to a systems security incident, including:

- to obtain professional (legal, public relations and IT forensics) advice, including assistance in managing the incident, coordinating response activities, making representation to regulatory bodies and coordination with law enforcement.
- to perform incident triage and forensic investigations, including IT experts to confirm and determine the cause of the incident, the extent of the damage including the nature and volume of data compromised, how to contain, mitigate and repair the damage, and guidance on measures to prevent reoccurrence.
- for crisis communications and public relations costs to manage a reputational crisis, including spokesperson training and social media monitoring.
- for communications to notify affected parties.
- for remediation services such as credit and identity theft monitoring to protect affected parties from suffering further damages.

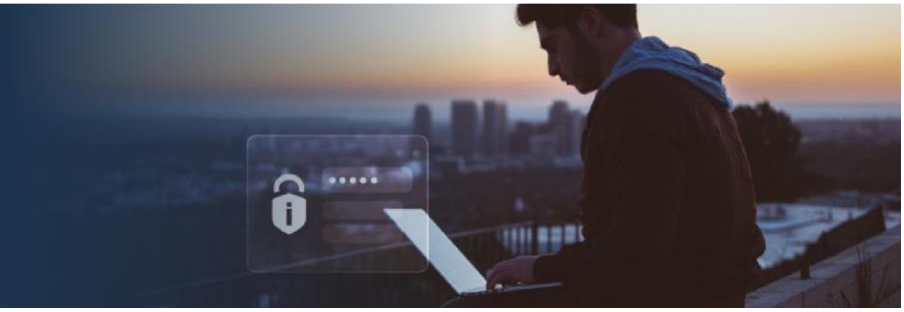
CYBER EXTORTION

Cyber extortion is a form of cybercrime in which attackers gain unauthorized access to a victim's systems, data, or network and threaten to release, damage, or disrupt unless a ransom is paid. Cyber extortion typically includes ransomware attacks, where attackers encrypt critical data and demand payment to decrypt it. Such incidents can cripple business operations, resulting in financial losses, reputational harm, and in some cases, the loss of crucial data.

Contact us

infosec@istorebusiness.co.za
https://www.istore.co.za/business-info-security
iStore Business

Core Peripherals (Pty) Ltd trading as iStore Business
Reg No: 1996/010298/07 | Vat No: 4190160756



IOT

An IoT (Internet of Things) event refers to any incident involving a device connected to the internet that collects, exchanges, or processes data. These events can include unauthorized access to or manipulation of IoT devices, such as smart home systems, industrial control systems, or wearable technology. IoT events pose unique security risks, as compromised devices can serve as entry points for larger cyber-attacks on networks and data.

The Warranty includes costs to respond to a systems security incident, including:

- to obtain professional (legal, public relations and IT forensics) advice, including assistance in managing the incident, coordinating response activities, making representation to regulatory bodies and coordination with law enforcement.
- to perform incident triage and forensic investigations, including IT experts to confirm and determine the cause of the incident, the extent of the damage including the nature and volume of data compromised, how to contain, mitigate and repair the damage, and guidance on measures to prevent reoccurrence.
- for crisis communications and public relations costs to manage a reputational crisis, including spokesperson training and social media monitoring.
- for communications to notify affected parties.
- for remediation services such as credit and identity theft monitoring to protect affected parties from suffering further damages.

BUSINESS EMAIL COMPROMISE

Business Email Compromise is the unrecoverable actual direct financial loss of money as confirmed by the relevant financial institution following the reasonable attempts for recovery, which belong to the business or for which the business is legally responsible, as a direct result of a Network Security Breach by a third party.

Reimbursement for the unrecoverable actual direct financial loss of money.