Liv Safe

Liberty General Insurance

# Safety tips against Cyber Risk

Issue 62nd
Volume 01
October 2020

**Cyber Technology** continues to develop in amazing, and sometimes alarming ways. Today, our personal relationships, work schedules and business decisions not only make use of but are reliant over cyber technology-based tools. Reliance over cyber technology makes us exposed to various risks.

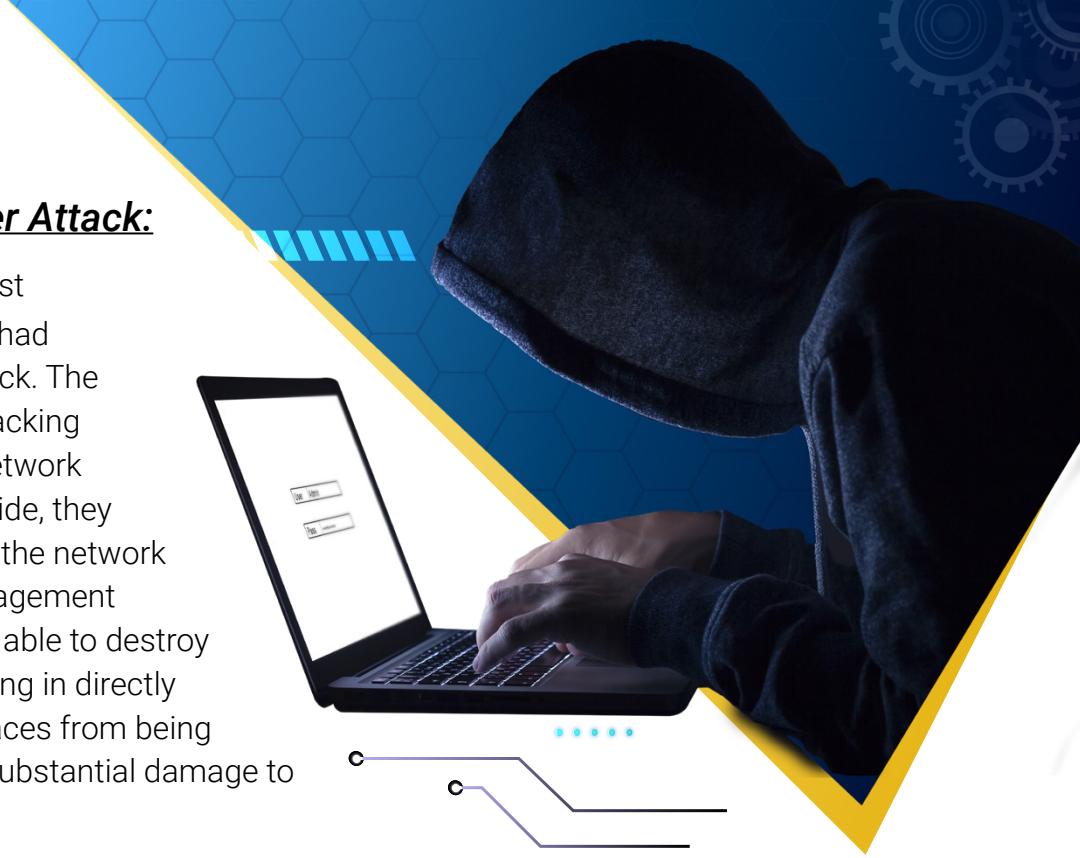
The world is looking for digital solutions to every field of work in an approach to become smart and sophisticated. Nearly every business faces cyber risk because of its associated service providers and employees who are connected to the Internet. The threat of becoming a victim of a cybercrime is increasing despite of various measures being incorporated by organisations.

We at Liberty General Insurance Limited understand the importance of cyber risk safety and consequences of being exposed to such risks. We intent to suggest some measures to cope up with such risks and hazards.

## Cyber Risk

Any risk associated with financial loss, disruption to operations or damage to an organisation's information and/or information systems using cyber technology as a tool can be termed as cyber risk. Examples includes data breaches, system outrages, thefts etc. As per an article published in "Economic Times" India ranks at 11th position in terms of number of cyber-attacks with 2,299,682 reported incidents in the 1st quarter of 2020.

# Case Studies



## *Manufacturing unit Cyber Attack:*

In the year 2014 one of the blast furnaces of German Steel Mill had been the victim of a cyber-attack. The attackers had done this by attacking into the corporate company network using malware. Then, once inside, they continued to navigate through the network to access the production management system. From there, they were able to destroy several control systems resulting in directly stopping one of the blast furnaces from being closed correctly and causing substantial damage to their manufacturing facility.

## *Cosmos Bank Cyber Attack:*

A cyber-attack was deployed on Cosmos Bank in Pune, India in 2018. This daring attack shook the whole banking sector of India when hackers siphoned off Rs. 94.42 crore from Cosmos Cooperative Bank Ltd. in Pune. Hackers hacked into the bank's ATM server and took details of many visa and rupee debit cardholders. Money was wiped off while hacker gangs from around 28 countries immediately withdrew the amount as soon as they were informed.

# Dominant Cyber Risks

**Malware:**
Also called as 'computer virus' in layman's terminology is an unwanted piece of programming or software that installs itself on a targeted system, causing unusual behaviour.

**Phishing Attacks:**
Sensitive information is fetched from end user through email or messages.

**Vishing:**
It is another form of phishing where urgent voice mails convince victims they need to act quickly to protect themselves from arrest or other risk.

**Traffic Interception:**
Also known as "eavesdropping," traffic interception occurs when a third-party "listens" to information sent between a user and host.

**Drive-by Attack:**
It refers to unintentional download of malwares in the system. The user does not have to do any thing in this case.

**Trojan Horse:**
Trojan malware attempts to deliver its payload by disguising itself as legitimate software.

**Social Engineering:**
A similar method to phishing though the attackers uses social media platforms for setting up cyber traps.

**Password Thefts:**
An unwanted third party manages to steal or guess your password and runs amok with the information.

**Water hole attack:**
Attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit.

**Ransomware:**
Ransomware installs itself on a user system or network. Once installed, it prevents access to functionalities (in part or whole) until a "ransom" is paid to third parties.

**MitM Attack:**
A Man-in-the-Middle attack occurs when a third-party hijacks a session between client and host.

**SQL Injection:**
These are essentially data manipulation malwares, implemented to access information which isn't meant to be available.

**Cross Site Attack:**
The malware is loaded over to a vulnerable website and it gets downloaded to end user once they use the targeted website.

**DDoS (Distributed Denial of Service):**
Malicious parties target servers an overload them with user traffic. The aim is to slowdown the processing of targeted user.

# Cyber Risk hazards

### 1 Third Party Exposure or Outsourced company access

Outsourcing of company access to third party companies can put the end user to risk.

### 2 Patch Management

Outdated software can create a breach in firewall posing the organisation to risk.

### 3 Cloud Vulnerability

The more we rely on the cloud for data storage, the higher the risk of a major breach.

### 4 Mobile Security

Mobile technology can be a significant asset to businesses, but it can also expose them to potential cyber security breaches.

### 5 Outdated Hardware

Not all threats to cyber security come from software. The pace at which software updates are released can make it difficult for the hardware to keep up. This, in turn, creates exposures that can put companies' data at risk.

### 6 Internet of Things

The Internet of Things (IoT) connects devices from all over the world through the internet. This allows a network of devices to store, send, and receive data. Hackers can exploit internet connectivity as an access point to steal data.

### 7 Bring Your Own Device (BYOD) Policies

BYOD policies can also leave companies exposed to serious cyber security breaches. Personal devices can be easier to hack than company devices, creating an opening for attackers to breach networks and compromise data.

# Tips to reduce Cyber attacks

- A proactive approach is the best defence. Often, a combination of caution and anti-virus is enough to avoid most malware concerns.
- Installed anti-virus and anti-spywares should be updated regularly.
- Encryption of data and use of VPN (Virtual Private Networks) is recommended.
- Strong passwords must be used for protecting data and devices, password sharing should be strictly restricted with periodical changing of passwords.
- Emails and messages must be read correctly and any suspicion on language, spelling errors, email id must be reported to concerned authorities immediately.
- A dedicated Cyber Cell (department) can be formed within organisation to train, make aware, alert and guide the workforce on suspicious or potential cyber-attacks.
- Implementation of smart and strong firewalls can safeguard system to a great extent.
- Downloading and surfing to suspicious websites and links should be restricted.
- Critical information such as passwords, OTPs, User Identity details should never be shared over telephonic conversations or mails.

# Trivia

**The first ever recorded cybercrime took place in 1820** when, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology.