TROXELL

CYBER RISKS BASICS

'CYBER RISK' The risk an organization takes on from failure of their IT systems making it susceptible to anything from financial losses to disruptions or damages to the organization.

CYBERCRIME Any criminal activity that involves a computer, networked device or a network. The two primary categories of cybercrime include advanced cybercrime, composed of attacks against computer software and hardware, and cyber-enabled crime, which encompasses "traditional" crimes that are committed over the internet.

TYPES OF CYBERCRIME:

- **Malware**

A category of cyber threats which include Trojan horses, viruses, and worms. These are software that are designed to cause damage to a computer or network. Malware is often used to steal information from individuals or businesses.

- **Ransomware**

A type of malware that prevents users from accessing their system or data until they pay a ransom to regain access.

- **Cross-site Scripting**

A type of injection in which an attacker takes advantage of security vulnerabilities and inserts malicious scripts (a list of executable commands) into web pages. Such insertions can be used to access cookies, session tokens, or other sensitive information retained by the browser and used with that site, or even rewrite the content of the webpage.

- **Denial-of-Service Attacks**

Attackers overload a machine or network by flooding the target with data or traffic, resulting in legitimate traffic being prevented from visiting using the target machine or network. Reason for these sorts of attacks include disruption or even extortion.

- **SQL Injection Attack**

The insertion of a SQL query (a query that programmers use as a language to request and hold data from and for a database) that are covertly injected into an entry field for execution. These insertions may allow attackers to read sensitive data, execute administration operations, or use commands to the operating system.

- **Password Attack**

A cyber-attack in which an attacker tries to crack a user's password to gain access to a computer or network. Attackers use programs that may employ a variety of methods to guess passwords.

- **Phishing**

Scammers use fraudulent communications - such as email or text - or a fake website to get people to share personal information such as usernames, passwords, credit card details, or Social Security numbers.

- **Session Hijacking and Man-in-the-middle Attacks**

An attacker intercepts and relays data sent between two parties, impersonating both sides of communication. The attacker may alter the communication between the two parties or simply monitor and steal information being sent between the two, such as account numbers and passwords.

SOURCE:
MARSHBERRY