Protect Yourself

Kaspersky Labs' study of cybersecurity revealed 758 million malicious cyber attacks and security incidents worldwide in 2018, with one third having their origin in the U.S.

Marriott kicked off 2019 with a record-setting breach when the hotel group announced that hackers accessed the records -- including some passport numbers and credit card information -- of up to 383 million guests.

A New Year's Eve ransomware attack crippled Travelex, forcing the world's largest chain of money-exchange shops to take its internal networks, consumer-facing websites and app offline for several weeks to stop the virus, *The Wall Street Journal* reported.

Cyber risk commonly refers to any risk of financial loss, disruption or damage to the reputation of an organization resulting from the failure of its information technology systems. Cyber risk could materialize in a variety of ways, such as:

- Deliberate and unauthorized breaches of security to gain access to information systems
- Unintentional or accidental breaches of security
- Operational IT risks due to factors such as poor system integrity

Poorly managed cyber risks can leave you open to a variety of cybercrimes, with consequences ranging from data disruption to economic ruin.

The **Dark Web** is that part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable. The Dark Web poses new and formidable challenges for law enforcement agencies around the world.

Ransomware is malicious software that infects your computer and displays messages demanding a fee to be paid in order for your system to work again. It has the ability to lock a computer screen or encrypt important, predetermined files with a password.

Malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

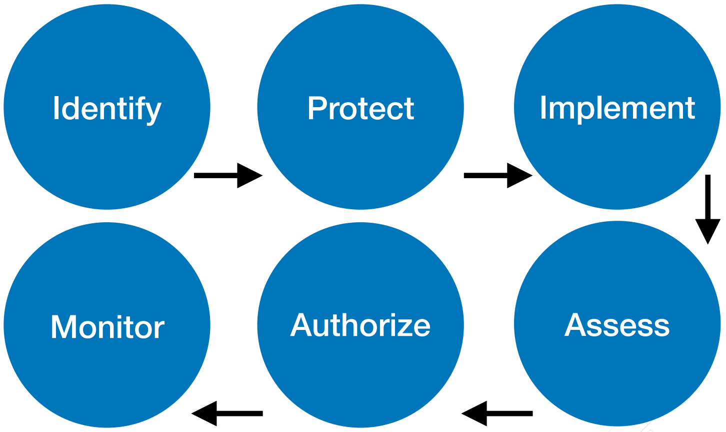
Employee Negligence is the primary cause of data breaches, according to ***Shred-it***, outpacing other forms of cyber attacks by a wide margin. According to the cybersecurity firm's survey of 1,000 business owners, 47 percent said that human error was responsible for a data breach in their organization, which was higher than any other cause.

Risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of occurrence of an event and its consequence.

With the rise of data storage and the expansion of technology, rules around privacy and protection are growing. Take for example new regulations like GDPR. The speed of technology is moving rapidly that changes must be put into place to protect customer information.

Cyber Risk

Compliance and Risk Management Plan



Identify → Protect → Implement ↓ Assess ← Authorize ← Monitor

Identify Identify your digital assets. evaluate not only the risk potential for data loss or theft but also prioritize the steps to be taken to minimize or avoid the risk associated with each type of data. The result of the Identify stage is to understand your top information security risks and to evaluate any controls you already have in place to mitigate those risks.

Protect Take steps to safeguard those assets. This includes a variety of processes, from implementing security policies to installing sophisticated software that provides advanced data risk management capabilities.

Implement Adopt formal policies and data security controls.

Assess Both existing and new security controls adopted by your business should undergo regular scrutiny.

Authorize Authorization examines not only who is informed, but what actions are taken, and how quickly.

Monitor Continuous monitoring and analysis are critical. Cyber thieves develop new methods of attacking your network and data warehouses daily. To keep pace with this onslaught of activity, you must revisit your reporting, alerts, and metrics regularly.

- NIST Compliance Manager
- Document Creation
- Office 365 and Azure Auditing, Security/Monitoring, and Backup
- Internal Threat Monitoring
- SIEM on UTM devices
- Security Awareness Training
- Endpoint Detection and Response
- Dark Web Monitoring
- Supplemental work to improve security via group Policy, File Server Ransomware kill switch, Office 365 security + compliance, Intune, and solutions within scope
- Triantan can assume role of vCISO

Triantan CCC, LLC

Triantan CCC, LLC
230 Spring Lake Drive
Itasca, Illinois 60143
877.282.9227
www.ccctechnologies.com