**Cyber security** is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks and technologies. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

**Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

**Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

**Information security** protects the integrity and privacy of data, both in storage and in transit.

### IoT (Internet of Things) security securing smart devices and networks that are connected to the IoT. IoT devices include things that connect to the Internet without human intervention, such as smart fire alarms, lights, thermostats and other appliances.

### Web security refers to the protective measures and protocols that organizations adopt to protect the organization from, cyber criminals and threats that use the web channel. Web security is critical to business continuity and to protecting data, users and companies from risk

## **Cyber security vs information security**

* Cyber security focuses on protecting computer systems from unauthorised access or being otherwise damaged or made inaccessible.
* Information security is a broader category that protects all information assets, whether in hard copy or digital form.

# **Features of Cyber Security**

### 1. Good analytics.

Every organization in every industry can benefit from good analytics. It’s easier to put your finger on a threat if you’ve rated your risks, and have a good historical picture of where your risks have been in the past. When you have good data, you can [clearly see your risk, monitor situations](https://securityscorecard.com/product/security-data) that could pose a threat, and move quickly when there’s an issue. In fact, good data can help you even after a data breach or attack. Ponemon’s 2019 Cost of A Data Breach report found that companies that use security analytics reduce the cost of data breaches by an average of $200,000.

#### **2. Coverage for external threats:**

According to the PurpleSec 2021’s report, around 27% of cyber attacks and incidents come from external sources. The external threats look like phishing, Denial of Services, vulnerable web applications, malicious email attachments, etc. Therefore, the security applications appended to the corporate system should continuously monitor such external threats. M.Sc. Cyber Security at IU International University of Applied Sciences will provide acute guidance on dealing with external threats.

### 3. A defense against internal threats.

While most of an organization’s threats tend to come from outside, occasionally the call is coming from inside the house. According to [Egress’s Insider Data Breach survey](https://www.egress.com/en-US/news/insider-data-breach-survey-2019-na), 95% of businesses are worried about an insider breach. This doesn’t necessarily mean you’ve got bad actors in your organization — most of the time internal threats are mistakes (like misconfiguration of AWS buckets or unapproved workarounds) or bad choices by employees. Occasionally, however, an internal actor will get involved with truly malicious activity like espionage or theft — Egress found that 61% of IT leaders believe their employees put sensitive company data at risk maliciously in the last year. Whatever their reasons for [exposing you to risk](https://securityscorecard.com/blog/top-cyber-security-threats-cisos-should-be-aware-of), a good cybersecurity platform should be able to quickly alert you to mistakes or misuse that could be putting your data or networks at risk.

### 4. Compliance.

Information security means different things in different industries. Every industry and organization — from healthcare to finance – has a unique set of regulations, standards, and best practices when it comes to information security. Your cybersecurity platform should help your organization [achieve, maintain and prove compliance](https://securityscorecard.com/solutions/use-cases/compliance) with whatever regulations are relevant to your industry and geographical location.

### 5. Manage risk across your entire ecosystem.

Third parties — your vendors, partners and contractors — are a [critical source of risk](https://securityscorecard.com/solutions/use-cases/third-party-risk-management) to your business. They often have access to your data and networks, but you can’t always require them to adhere to specific standards or best practices. It’s no surprise that third parties are a significant source of risk — Ponemon’s 2019 Cost of A Data Breach report found that when third parties cause a breach, the cost increases by more than $370,000. Yet, according to Protoviti’s [2019 Vendor Risk Management Benchmark Study](https://www.protiviti.com/US-en/insights/vendor-risk-management), only 4 in 10 organizations have a fully mature vendor risk management process in place. Your cybersecurity platform should let you monitor and [manage the risks posed by your vendors](https://securityscorecard.com/blog/tips-for-managing-supply-chain-cybersecurity-risk). Your cybersecurity platform must allow you to monitor and manage risk no matter where it occurs — outside the company, inside your organization, or in your supply chain.

#### **6. Threat detection, prevention, and response:**

According to the survey published by CISO magazine, 35 percent of CISO professionals want an all-inclusive security system that can block almost all (95 out of 100) attacks. Furthermore, they also want that platform to track and provide a spontaneous alert for those attacks that it cannot block. MS Cyber Security or M.Sc. Cyber Security aspirants get training to track down such suspicious activities and eliminate them. They use tools like hardware and software firewalls, network analyzers, SSL/TLS proxy servers, and other apps to detect and prevent breaches.

### 7. Continuous monitoring.

When it comes to cybersecurity, it’s [no good relying on snapshot](https://securityscorecard.com/blog/vendor-risk-assessments-continuous-monitoring)s of your risk, or compliance. Yes, you and your vendors might be compliant right now, but tomorrow, a patch might not be installed in a timely manner, or someone might misconfigure a server. A security platform that doesn’t provide [continuous monitoring](https://securityscorecard.com/blog/benefits-continuous-compliance-monitoring-in-cloud) is leaving holes in your compliance and leaving you open to risk.

## **Principles of Cyber Security**

## The primary objective of cyber security is to protect data. The security community commonly refers to a triangle of three related principles that ensure data is secure, known as the CIA triad:

* **Confidentiality**— ensuring sensitive data is only accessible to those people who actually need it, and are permitted to access according to organizational policies, while blocking access to others.
* **Integrity**— making sure data and systems are not modified due to actions by threat actors, or accidental modification. Measures should be taken to prevent corruption or loss of sensitive data, and to speedily recover from such an event if it occurs.
* **Availability**— ensuring that data remains available and useful for its end-users and that this access is not hindered by system malfunction, cyber-attacks, or even security measures themselves.

There are some terms use in cyber security

**Virus:** A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

[**Trojans**](https://www.kaspersky.co.in/resource-center/threats/trojans)**:**A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computers where they cause damage or collect data.

**Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

**Ransomware:** Malware which locks down a user’s files and data, with the threat of erasing it unless a ransom is paid.

**Adware:** Advertising software that can be used to spread malware.

**Botnets:** Networks of malware infected computers which cybercriminals use to perform tasks online without the user’s permission.

[**Zero-day exploit**](https://www.imperva.com/learn/application-security/zero-day-exploit/): A first attempt to perform a cyber attack by exploiting a security vulnerability in a computer system. Because the vulnerability is not yet known, the attack is highly likely to succeed.

**SQL injection:**An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

**Phishing**: [Phishing](https://www.kaspersky.co.in/resource-center/threats/spam-phishing) is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

**Man-in-the-middle attack**: A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim’s device and the network.

**Denial-of-service attack**: A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

**C**[**ode injection**](https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/): An attempt by attackers to send malicious code to a computer system and cause it to process and execute that code. Common variants are SQL Injection and Cross-Site Scripting (XSS).