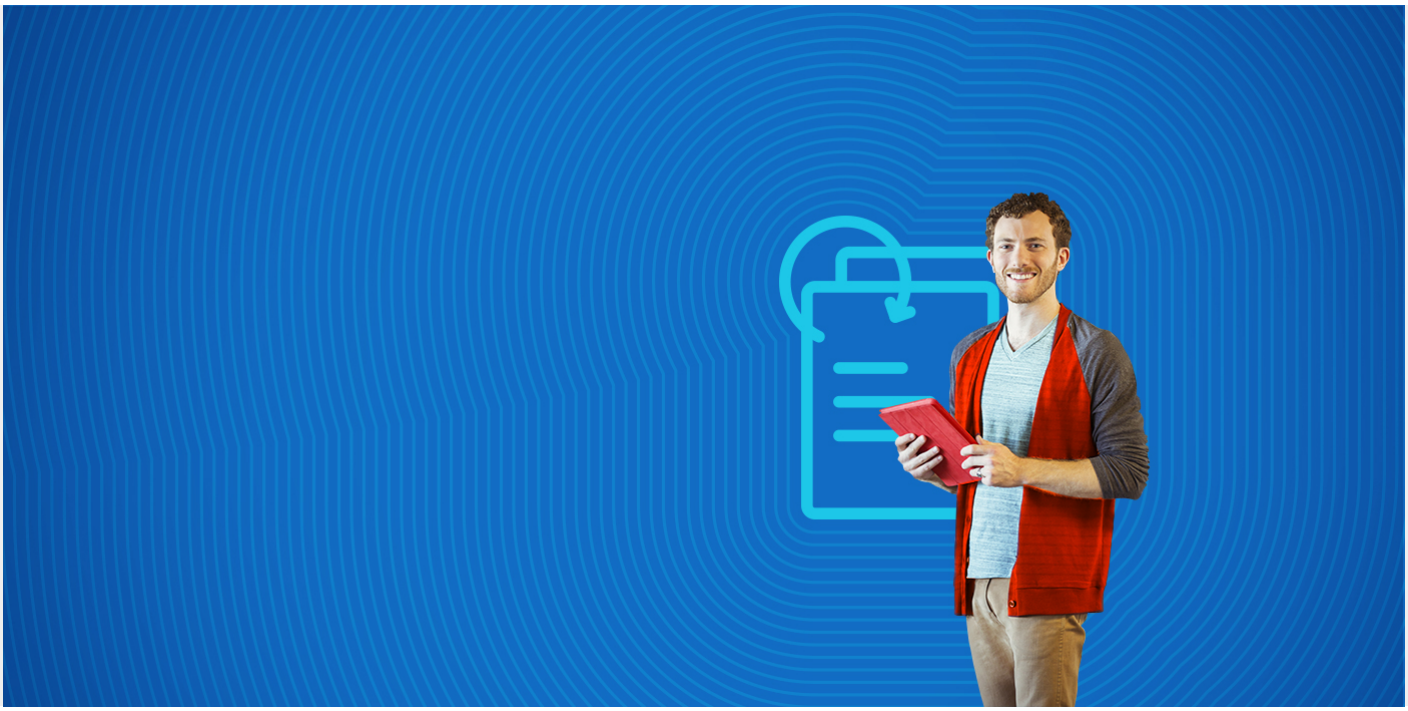
CYBERSECURITY: A BEGINNER'S GUIDE



Cybersecurity is the process of protecting data, electronic systems, and networks against cyber threats. These threats might have any aim: gaining unauthorized access, creating damage, or compromising digital information, services, and resources—perhaps for financial or political gain.

This primer on cybersecurity will define the concept and cybersecurity types, look at recent trends, and provide best practices and additional resources on maintaining cybersecurity.

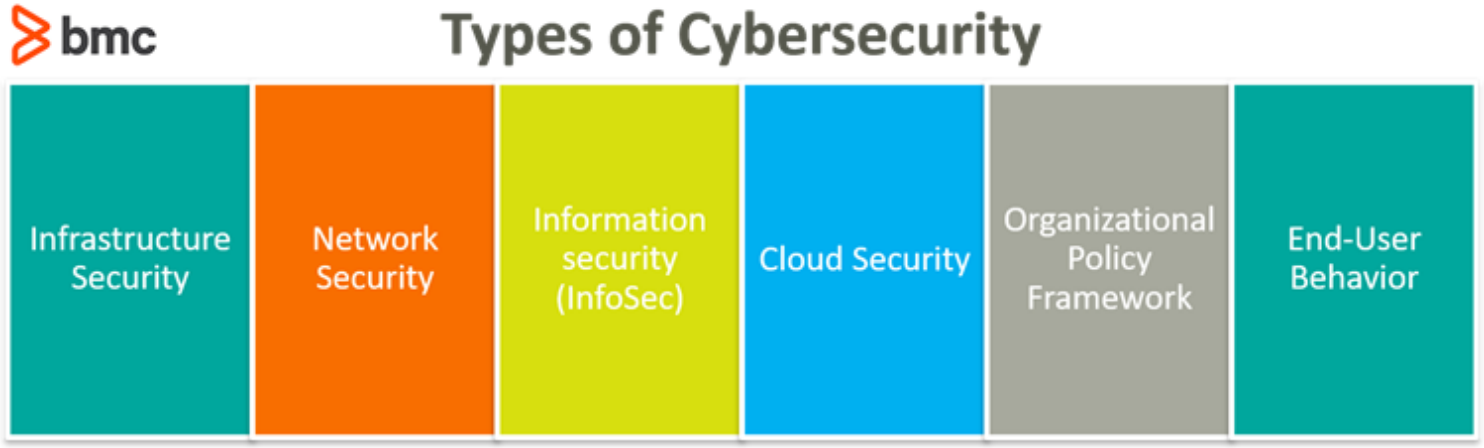
What is cybersecurity?

The goal of cybersecurity initiatives is to maintain the integrity, confidentiality, and availability of your data assets and technologies. A subset of IT security, cybersecurity is focused primarily on the security of digital assets against digital attack vectors. An effective cybersecurity strategy encompasses the technologies, end-user practices, and processes that can affect your digital asset security.

Cybersecurity involves the use of advanced technology solutions for detecting, mitigating, and remediating against cyber-attacks. Additionally, cybersecurity principles include security-aware end-user and organizational behavior, as well as policy frameworks for timely identification and effective response to cyber-attacks.

Types of cybersecurity

Cybersecurity can be applied to a variety of categories across the technology stack, from user-facing applications and backend network infrastructure to organizational policies and end-user behavioral practices. Here are the most common categories of cybersecurity:



Infrastructure Security

Relates to the security of utility services infrastructure use to power and operate datacenter technologies, cloud, and networks. A cyber-attack causing power outages at datacenters are often aimed at its critical utility infrastructure systems. Examples of this infrastructure include:

- Power supply and transmission systems
- Water supply and cooling
- Heating and ventilation
- Other cyber-physical systems

Network Security

Data must be secured during transmission. Network security measures such as encryption, traffic monitoring, firewalls, Virtual Private Networks (VPNs), and end-point security ensure data integrity as it transmits between servers and clients across distributed networks.

Information Security (InfoSec)

Involved with the security of data across its end-to-end lifecycle, InfoSec measures are designed to ensure that only the authorized users, apps, and systems are able to access the required information. The main objectives of information security include confidentiality, integrity and availability (CIA) of data. Additional objectives include accountability and authenticity of information, which contribute to the overall security and privacy associated with digital information.

Cloud Security

Digital information, apps, and services typically reside in servers across geographically distributed data centers accessed over Internet networks. These data centers, known as cloud systems, should be secure and designed to meet Service Level Agreement (SLA) objectives as decided between cloud vendors and its customers. Cloud security ensures that this infrastructure and the data stored in cloud systems is secure against cyber threats. Other objectives include that privacy and service availability is ensured within a network of shared cloud infrastructure resources.

Organizational Policy Framework

Your organizational policy framework is the part of cybersecurity responsible for mitigating security risks. It relates to everything, ranging from the choice of cybersecurity solutions, access controls and privileges assigned to end-users, disaster response, and preparation. The policy framework should be designed as an optimal tradeoff between security, cost, performance and business value of cybersecurity initiatives.

End-User Behavior

Users are the first line of defense against cyber-attacks. Many security vulnerabilities in technologies and systems can be addressed by controlling the human element compromised with a cyber-attack. Educating users about the security best-practices such as regularly updating systems for security, keeping strong passwords and authentication systems, and not exposing critical corporate information and digital workloads to security-prone IT environments and situations is the first step for any cybersecurity program.

Cybersecurity trends

Cyber threats come in various forms. Organizations use all kinds of sophisticated technologies to protect sensitive digital assets. At the same time, cybercrime underground rings with seemingly endless resources continue to exploit unpatched system vulnerabilities and unsuspecting users. The result is devastating for corporate organizations, governments and end-users alike. The global cybersecurity market is worth $173 billion in 2020 and expected to reach $270 billion by the year 2026.

Despite the improving security systems in place, many organizations fail to prepare against overwhelming security threats and succumb to the attacks. Consider the following trends observed in the year 2019:

- On average, only 5% of data folders in corporate computer systems are adequately protected. (Varonis)
- 1 billion data records were exposed in the first six months of the year 2019. (RiskBased)
- A cyber-attack is performed every 39 seconds, 2,244 times a day. (University of Maryland)
- The average cost of data breach is $3.92 million. (Security Intelligence)
- 53% of companies had over 1,000 sensitive files accessible to every employee. (Varonis)
- 43% of security incident victims were small business organizations. (Verizon)
- Cybersecurity unemployment is 0%, with related job postings expected to increase by 32% between 2018-2028. (CSO Online, Bureau of Labor Statistics)

Creating a cybersecurity strategy

So how do you maintain security of sensitive digital assets? These assets are your competitive differential, but they that also obligate you to protect end-user privacy. Note the following actions and considerations when developing your cybersecurity strategy:

1. **Not all data assets and infrastructure resources should be protected in the same way.** Each digital asset has an associated business value and privacy requirement. Optimize your cybersecurity investments to protect the most critical digital assets.

2. **Identify and map your digital assets.** Apply cybersecurity protocols across the taxonomy of digital assets with a strategic perspective. Assess the risk across different levels of your digital asset portfolio. Locate the dependencies and establish appropriate data security, redundancy and disaster recovery mechanisms.
3. **High spending doesn't guarantee better cybersecurity.** Even the most expensive technology solutions can potentially fail when hackers compromise the human element and gain access to sensitive data impersonating legitimate users.
4. **Threats come from within your organization itself.** Recent research indicates that insider threats are responsible for 50% of all cybersecurity incidents—that's half of all your incidents! These insider threats can be employees demonstrating negligent behavior against security risks as well as those with malicious intent.
5. **Establish a culture of security awareness.** Employees access sensitive IT services and data and must be educated over the necessary security best practices.
6. **Educate corporate leadership about cybersecurity risks and strategic best-practices.** From a strategic perspective, corporate leadership should help develop an optimal tradeoff between business and security performance of their cybersecurity strategy.
7. **Focus on establishing a resilient security posture.** Investments into cybersecurity solutions shouldn't be seen as silver bullets; instead, the ability to understand the risk, react proactively and mitigate risks across the lifecycle of a cybersecurity incidents makes the organization secure against rising threats.

Additional resources

For more information on cybersecurity at the enterprise level, check out these BMC Blogs:

- Big Data Security Issues in the Enterprise
- How to Apply Machine Learning to Cybersecurity
- The Secret Life of Your Network: 9 Threats Lurking in Your Data Center
- Cybersecurity Incident Response on the Mainframe
- The Mainframe Security Intelligence Gap
- Leveraging Automation to Bridge the Cybersecurity Skills Gap and Secure Your Mainframe Data
- Top IT Security, InfoSec, & CyberSecurity Conferences of 2020