***What is cybersecurity?***

Cybersecurity is the state or process of protecting and recovering computer systems, networks, devices, and programs from [any type of cyber-attack](https://www.upguard.com/blog/cyber-attack). Cyber-attacks are an increasingly sophisticated and evolving danger to your sensitive data, as attackers employ new methods powered by social engineering and artificial intelligence to circumvent traditional security controls.

Cybersecurity risk is increasing, driven by global connectivity and usage of cloud services, like Amazon Web Services, to [store sensitive data](https://www.upguard.com/blog/sensitive-data) and personal information. Widespread [poor configuration of cloud services](https://www.upguard.com/blog/check-your-amazon-s3-permissions-someone-will) paired with increasingly sophisticated cyber criminals means the risk that your organization suffers from a successful cyber-attack or [data breach is on the rise](https://www.upguard.com/blog/data-breach).

Gone are the days of simple firewalls and antivirus software being your sole security measures. Business leaders can no longer leave information security to cybersecurity professionals.

Cyber threats can come from any level of your organization. You must educate your staff about simple social engineering scams like [phishing](https://www.upguard.com/blog/phishing) and more sophisticated cybersecurity attacks like [ransomware attacks](https://www.upguard.com/blog/ransomware) (think [WannaCry](https://www.upguard.com/blog/wannacry)) or other [malware](https://www.upguard.com/blog/malware) designed to steal intellectual property or personal data.

The fact of the matter is the world is increasingly reliant on technology and this reliance will continue as we introduce the next generation of smart Internet-enabled devices that have access to our networks via Bluetooth and Wi-Fi.

***The importance of cybersecurity:***

Cybersecurity's importance is on the rise. Fundamentally, our society is more technologically reliant than ever before and there is no sign that this trend will slow. Personal data that could result in identity theft is now posted to the public on our social media accounts. Sensitive information like social security numbers, credit card information and bank account details are now stored in cloud storage services like Dropbox or Google Drive.

Cybersecurity is important because it encompasses everything that pertains to protecting our sensitive data, [personally identifiable information (PII)](https://www.upguard.com/blog/personally-identifiable-information-pii), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems from theft and damage attempted by criminals and adversaries

***Why is cybercrime increasing?***

Information theft is the most expensive and fastest growing segment of cybercrime. Largely driven by the increasing exposure of identity information to the web via cloud services. But it is not the only target. Industrial controls that manage power grids and other infrastructure can be disrupted or destroyed. And identity theft isn't the only goal, cyber-attacks may aim to compromise data integrity (destroy or change data) to breed distrust in an organization or government.

Cybercriminals are becoming more sophisticated, changing what they target, how they affect organizations and their methods of attack for different security systems.

[Social engineering](https://www.upguard.com/blog/social-engineering) remains the easiest form of cyber attack with ransomware, [phishing, and spyware](https://www.upguard.com/blog/spyware) being the easiest form of entry. Third-party and fourth-party vendors who process your data and have poor cybersecurity practices are another [common attack vector](https://www.upguard.com/blog/attack-vector), making [vendor risk management](https://www.upguard.com/blog/vendor-risk-management) and [third-party risk management](https://www.upguard.com/blog/third-party-risk-management-framework) all the more important.

Other factors driving the growth in cybercrime include:

* The distributed nature of the Internet
* The ability for cybercriminals to attack targets outside their jurisdiction making policing extremely difficult
* Increasing profitability and ease of commerce on the [dark web](https://www.upguard.com/blog/dark-web)
* The proliferation of mobile devices and the Internet of Things.

***What is the impact of cybercrime?***

A lack of focus on cybersecurity can damage your business in range of ways including:

* Economic costs: Theft of intellectual property, corporate information, disruption in trading and the cost of repairing damaged systems
* Reputational costs: Loss of consumer trust, loss of current and future customers to competitors and poor media coverage
* Regulatory costs: GDPR and other data breach laws mean that your organization could suffer from regulatory fines or sanctions as a result of cybercrimes

Given the nature of cybercrime and how difficult it can be to detect, it is difficult to understand the direct and indirect costs of many security breaches. This doesn't mean the reputational damage of even a small data breach or other security event is not large. If anything, consumers expect increasingly sophisticated cybersecurity measures as time goes on.

***Examples of damages to companies affected by cyber-attacks and data breaches***

The number of cyber-attacks and data breaches in the recent years is staggering and it's easy to produce a laundry list of companies who are household names that have been affected.

Here's a few examples:

* Equifax: The Equifax cybercrime identity theft event affected approximately 145.5 million U.S. consumers along with 400,000-44 million British residents and 19,000 Canadian residents. Equifax shares dropped 13% in early trading the day after the breach and numerous lawsuits were filed against Equifax as a result of the breach. Not to mention the reputational damage that Equifax suffered. On July 22 2019, Equifax agreed to a settlement with the FTC which included a $300 million fund for victim compensation, $175m for states and territories in the agreement and $100 million in fines.
* eBay: Between February and March 2014, eBay was the victim of a breach of encrypted passwords, which resulted in asking all of its 145 million users to reset their password. Attackers used a small set of employee credentials to access this trove of user data. The stolen information included encrypted passwords and other personal information, including names, e-mail addresses, physical addresses, phone numbers and dates of birth. The breach was disclosed in May 2014, after a month-long investigation by eBay.
* Yahoo: Yahoo disclosed that a breach in August 2013 by a group of hackers had compromised 1 billion accounts. In this instance, security questions and answers were also compromised, increasing the risk of identity theft. The breach was first reported by Yahoo on December 14, 2016, and forced all affected users to change passwords, and to renter any unencrypted security questions and answers to make them encrypted in the future. However, by October of 2017, Yahoo changed the estimate to 3 billion user accounts. An investigation revealed that users' passwords in clear text, payment card data and bank information were not stolen. Nonetheless, this remains one of the largest data breaches of this type in history.

While these are a few examples of high-profile data breaches, it's important to remember that there are even more that never made it to the front page.

***How to protect your organization against cybercrime:***

There are three simple steps you can take you increase security and reduce risk of cybercrime:

1. Educate all levels of your organization about the risks of social engineering and common social engineering scams like phishing emails and [typo squatting](https://www.upguard.com/blog/typosquatting)
2. Invest in tools that limit information loss, monitor your [third-party risk](https://www.upguard.com/articles/five-things-to-know-about-third-party-risk) and [fourth-party vendor risk](https://www.upguard.com/blog/what-is-fourth-party-risk) and continuously scan for data exposure and leak credentials
3. Use technology to reduce costs like automatically sending out [vendor assessment questionnaires](https://www.upguard.com/articles/planning-your-vendor-security-assessment-questionnaire) as part of an overall [cyber security risk assessment](https://www.upguard.com/blog/cyber-security-risk-assessment) strategy