What is Cybersecurity?

What is Cybersecurity

- Improve your ability to keep yourself cyber-secure.
- It means quite different things to different people in different situations.
- Technically speaking, cybersecurity is the subset of information security that addresses information and information systems that store and process data in electronic form.
- On the other hand, information security encompasses the security of all forms of data (for example, securing a paper file and a filing cabinet).

Cybersecurity Means Different Things to Different Folks

- **For individuals**, cybersecurity means that their personal data is not accessible to anyone other than themselves and others they have authorized, and that their computing devices work properly and are free from malware.
- **For small business owners**, cybersecurity may include ensuring that credit card data is properly protected and that standards for data security are properly implemented at point-of-sale registers.
- **For firms (companies) conducting online business**, cybersecurity may include protecting servers that untrusted outsiders regularly interact with.
- **For shared service providers**, cybersecurity may entail protecting numerous data centers that house numerous servers that, in turn, host many virtual servers belonging to many different organizations.
- **For the government**, cybersecurity may include establishing different classifications of data, each with its own set of related laws, policies, procedures, and technologies.

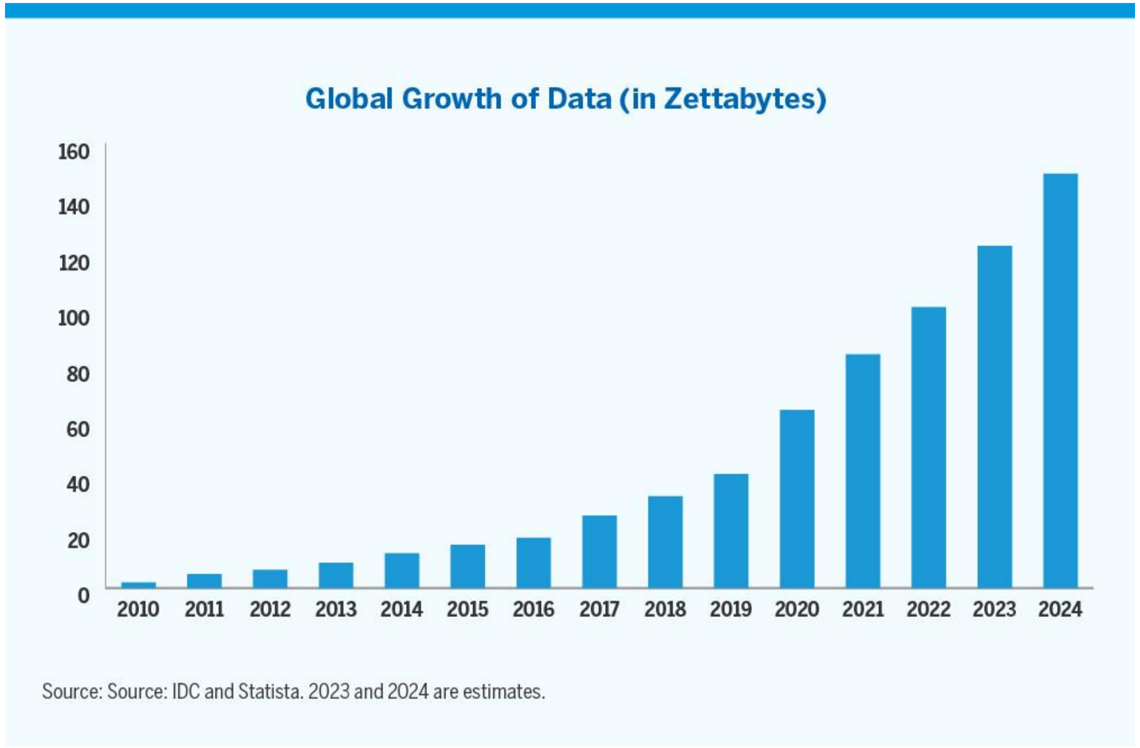
Cybersecurity Is a Constantly Moving Target

The ultimate goal of cybersecurity may not change much over time.

However, the policies, procedures, and technologies used to achieve its goal change dramatically over time.

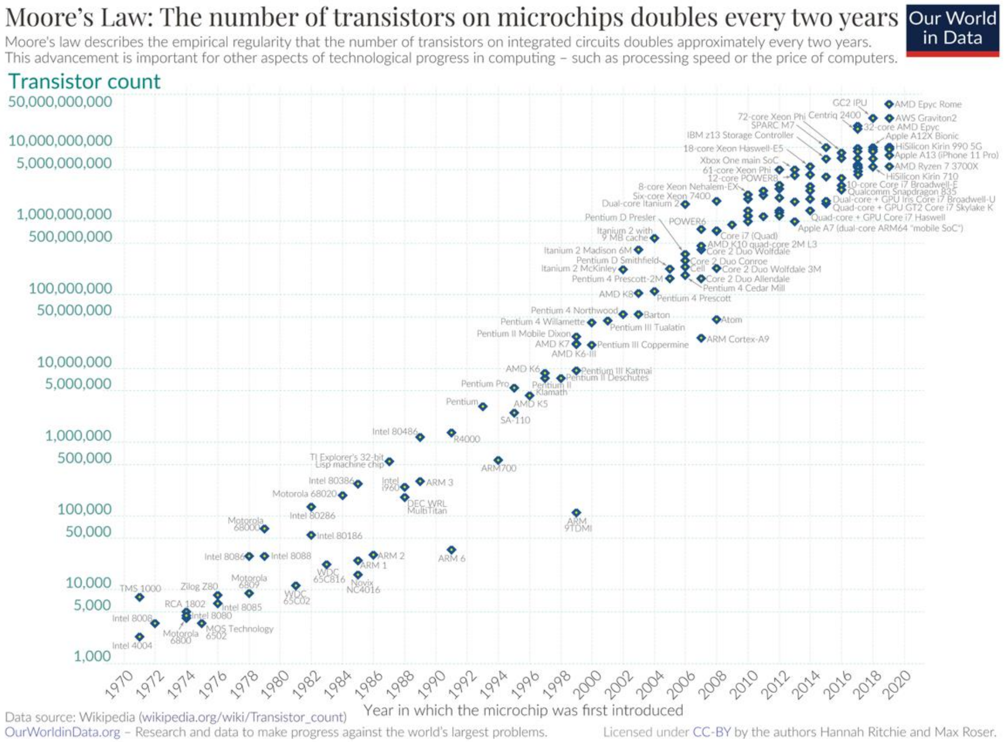
Many approaches and technologies that were more than adequate to protect consumers’ digital data in 1980, for example, are effectively worthless today.

Digital Revolution



Global Growth of Data (in Zettabytes)

Source: Source: IDC and Statista. 2023 and 2024 are estimates.



Moore's Law: The number of transistors on microchips doubles every two years

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years.
This advancement is important for other aspects of technological progress in computing – such as processing speed or the price of computers.

Data source: Wikipedia (wikipedia.org/wiki/Transistor_count)
OurWorldinData.org – Research and data to make progress against the world's largest problems.

Technological changes: Digital data

- **Shift from Physical to Digital Data**: Traditional physical data security (locked cabinets, limited access) has been replaced by complex digital systems that require automated authentication, access control, and real-time threat protection from anywhere.
- **Increased Data Vulnerability**: The transition to digital communication (email, chat) and media (photos, videos) has moved vast amounts of sensitive information to internet-connected servers, creating new opportunities for theft, ransom attacks, and misuse.
- **Expanded Attack Surface**: The digital landscape exposes data to various threats, including data breaches, ransomware, copyright infringement, and personal privacy violations.

Technological changes: The Internet

- **Internet's Transformation & Expanded Reach**: The Internet has evolved from a small research network into a global communication system connecting billions of **people**, **devices**, and **industrial control** systems, creating unprecedented opportunities for malicious actors
- **New Cyber Threats and Risks**: The interconnected nature of the Internet has enabled attackers to **disrupt businesses, manipulate elections, cause infrastructure failures, and steal large sums of money remotely**, scenarios previously unimaginable.
- **Monetization of Cybercrime**: The advent of online banking and commerce has made cybercrime more profitable, attracting more individuals and groups and escalating the scope and impact of cyberattacks.

Technological changes: Cryptocurrency

- Crypto Makes Cybercrime Easier: Cryptocurrency has made it much easier and more profitable for cybercriminals to make money.

- Hiding Money is Easier: Criminals can now hide their money better because it's harder to track cryptocurrency payments back to them.

- More Money, More Crime: With more crypto wealth, criminals can buy better tools and trick people into fake crypto investments. It also helps them hide money from other crimes.

Technological changes: Mobile workforces and universal access

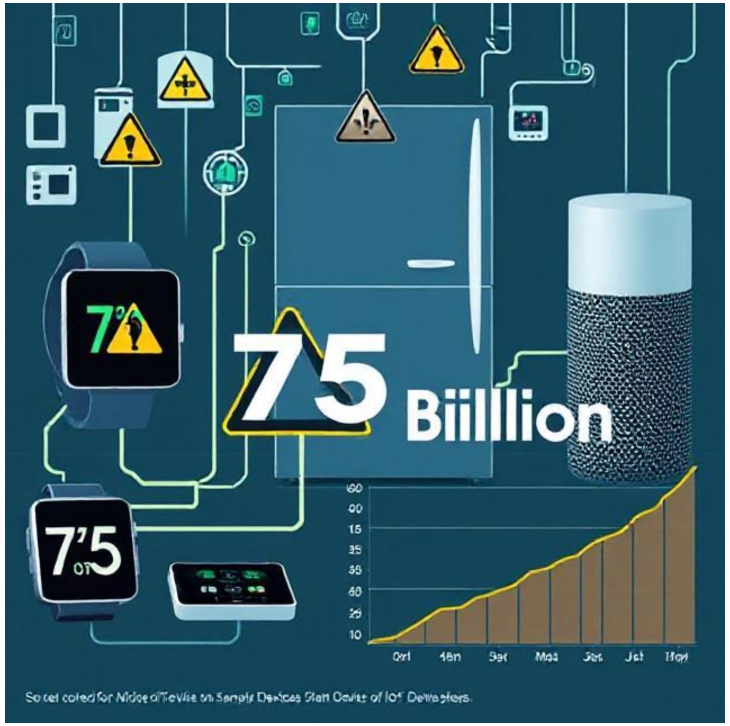
- **Old Security, Limited Access**: In the past, company networks were closed off. Employees had limited or no remote access, making it hard for hackers to get in.

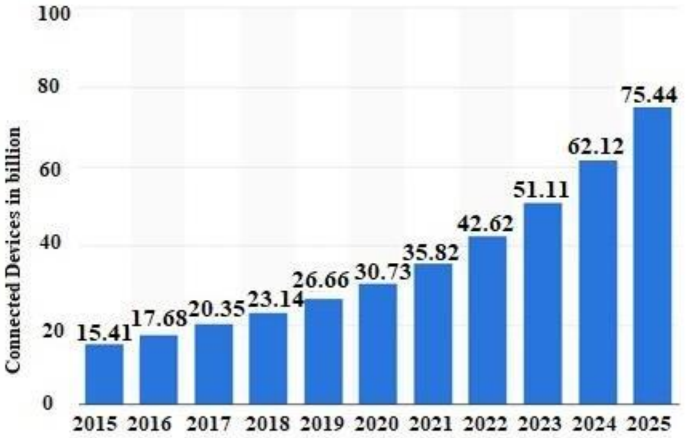
- **Internet Changed Everything**: While the Internet created some risk, firewalls mostly kept internal systems separate.

- **Remote Access & Mobile Work**: New Risks Remote access tools like VPNs and affordable mobile internet have made it easier to work from anywhere. But this also makes it easier for hackers to access sensitive data, so security needs to be updated.

Technological changes: Smart Devices

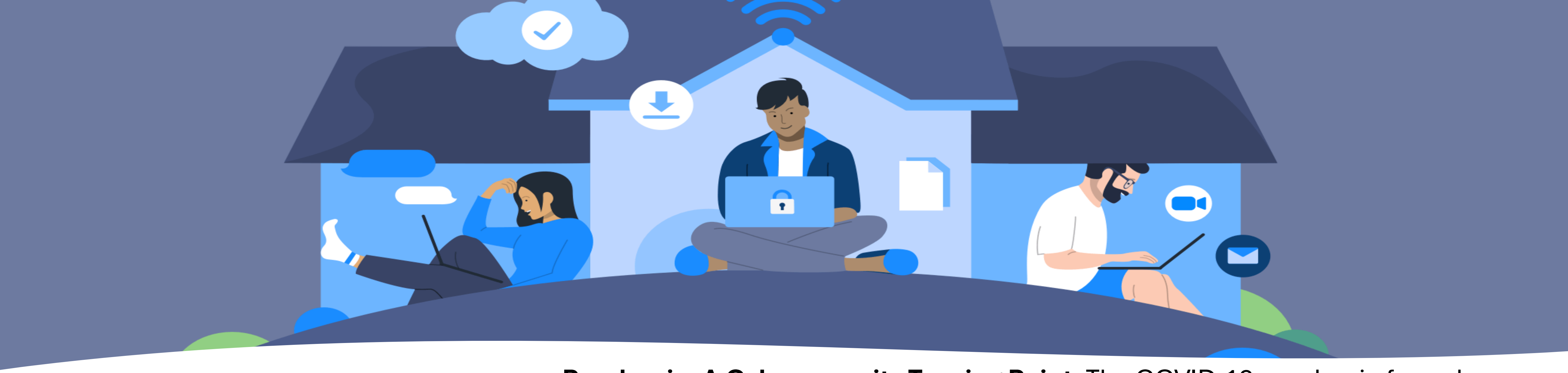
- **Smart Devices Everywhere**: The number of "smart" devices connected to the internet (like appliances and gadgets) is growing at an explosive rate. By 2025, it's estimated that there will be over 75 billion IoT devices worldwide, creating countless new entry points for cyberattacks.
    - https://www.statista.com/statistics/1194701/iot-connected-devices-use-case/
    - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3619450
- **New Entry Points for Hackers**: These smart devices can be hacked and controlled remotely, making our lives less secure.
- **Cheap Devices, Hidden Risks**: We can easily buy cheap smart devices from anywhere in the world, but they might have hidden security problems that put our information at risk.





Technological changes: Big Data

- **Double-Edged Sword**: While helping create better cybersecurity tools, big data also provides attackers with valuable information.
- **Easier Social Engineering**: By analyzing large amounts of data about employees, criminals can more easily trick their way into organizations. Studies show that over 90% of cyberattacks start with some form of social engineering.
- **Privacy Concerns & Control**: Companies are forced to implement strict data controls to prevent leaks, leading to concerns about data misuse and privacy violations.

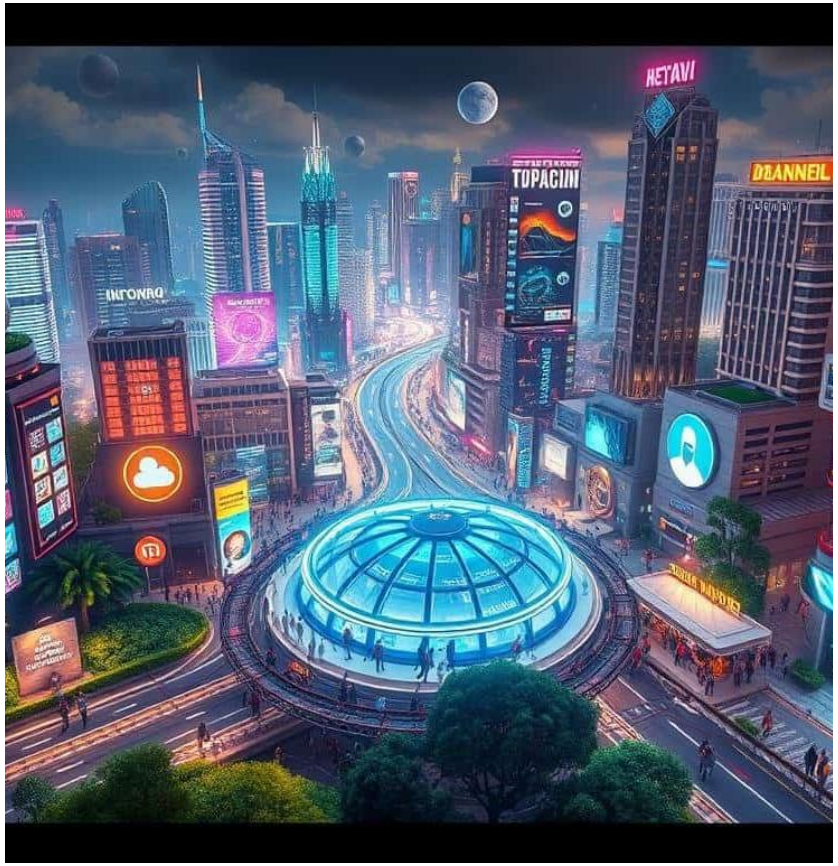


Technological changes: The COVID-19 pandemic

- **Pandemic, A Cybersecurity Turning Point**: The COVID-19 pandemic forced a massive shift to remote work, creating significant and lasting cybersecurity challenges
- **Unprepared Infrastructure**: Many organizations lacked the infrastructure and security measures to support widespread remote work, leaving them vulnerable. A study found that 68% of organizations experienced a cybersecurity incident related to remote work during the pandemic.
  - https://www.netwrix.com/download/collaterals/2021%20Netwrix%20Sysadmin%20Report%20July.pdf
- **New Vulnerabilities**: Remote meetings, social engineering attacks, distractions, and stressed employees created new opportunities for hackers.
- **Inadequate Equipment**: Due to the urgent switch, some organisations could not provide employees with secure working equipment, causing them to rely on unsecured personal devices.

Technological changes: Social Shift

- **Connected World:** The Internet allows global interaction but also enables global crime.
- **Accessibility Creates Vulnerability**: The shift to digital information accessible from anywhere increases the amount of data hackers can steal.
- **Social Media & Oversharing**: People share more information online, making it easier for criminals to gather information for social engineering attacks.
  - https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/
- **Pressure to Convert**: The expectation of constant access to data forces organizations to move sensitive information online, creating more opportunities for criminals.



Technological changes: Economic model shifts

- **Globalized Outsourcing**: The internet enables cost-effective outsourcing of tasks like software development and customer service to locations worldwide, a common practice.
- **Increased Cybersecurity Risks**: This shift creates vulnerabilities in data transmission, intellectual property protection, and code integrity.
- **Backdoor Concerns**: Software and hardware developed in foreign countries could contain intentional or unintentional backdoors, posing a significant threat.
- **Need for Stronger Protection**: Enhanced cybersecurity measures are crucial to protect against data theft and modification and ensure the security of outsourced operations.

Political shifts: Data collection

- Governments can now spy on citizens globally on an unprecedented scale due to digital information proliferation.
- Reduced storage costs and advancing technologies motivate governments to collect and store vast amounts of personal data.
- Expected advancements in quantum computing could compromise current encryption, enhancing government data access.
- Businesses must protect data to prevent hostile nations from using it for intelligence or malicious purposes.

Political shifts: Election interference

- Election interference, historically costly and risky, is now easier and more effective due to social media's reach and low cost.
- Misinformation campaigns spread rapidly, stirring up civil unrest and undermining trust in election integrity.
- Electronically stored voter registration databases are vulnerable to remote manipulation, even if rarely successful.
- Concerns over election integrity, exacerbated by insecure mail-in ballots, fuel mistrust across the political spectrum.

Political shifts: Hacktivism

- A Product of Globalization and Digital Connection
- The spread of democracy and internet connectivity has ushered in an era of hacktivism.
- Increased global awareness allows individuals to target governments or citizens from afar.
- Motivations range from anger over government policies to disagreement with another country's actions.

Political shifts: Greater freedom

- Freedom's Double Edge: The Internet's Impact on Repressive Regimes.
- Increased awareness of lifestyles in freer countries is driving pressure for liberalization in repressed societies.
- Some governments respond by implementing cybersecurity controls to restrict access to internet-based services.

Political shifts: Sanctions

- Sanctioned states are increasingly using cybercrime to circumvent economic restrictions.
- North Korea, for example, uses cryptocurrency mining malware to generate revenue.
- Inadequate individual cybersecurity can have a direct impacts on international political negotiations.

Political shifts: New balances of power

- Patching gaps can easily undermine an otherwise strong system.
- Cybercriminals face dramatically lower risk of arrest and prosecution compared to other criminals.
- Law enforcement often lacks the resources to track down and prosecute cybercriminals operating across borders.
- The low cost, high potential reward, and minimal risk make cybercrime highly attractive to criminals.

Your questions?