

# Introduction to Cyber Security

---

Vathna.lay@cadt.edu.kh

---

# What is Exactly is Cyber Security?



# Cyber Security



Individuals



Small Business  
Owners



Online Business



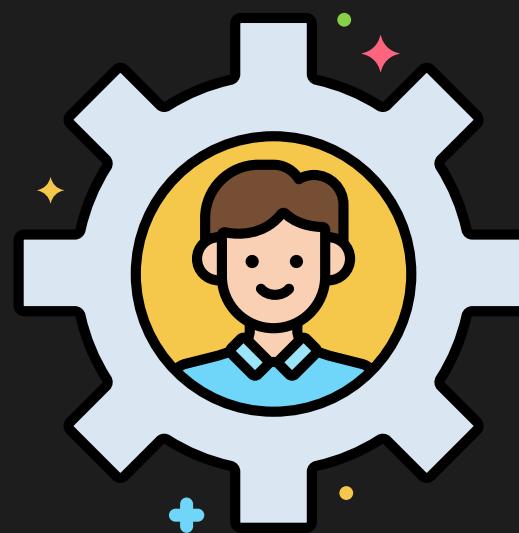
Service Provider



Government



# Cyber Security (Individuals)



Individuals

Cybersecurity means authorized access to personal data and malware-free devices.

2024



# Cyber Security (Small Business)



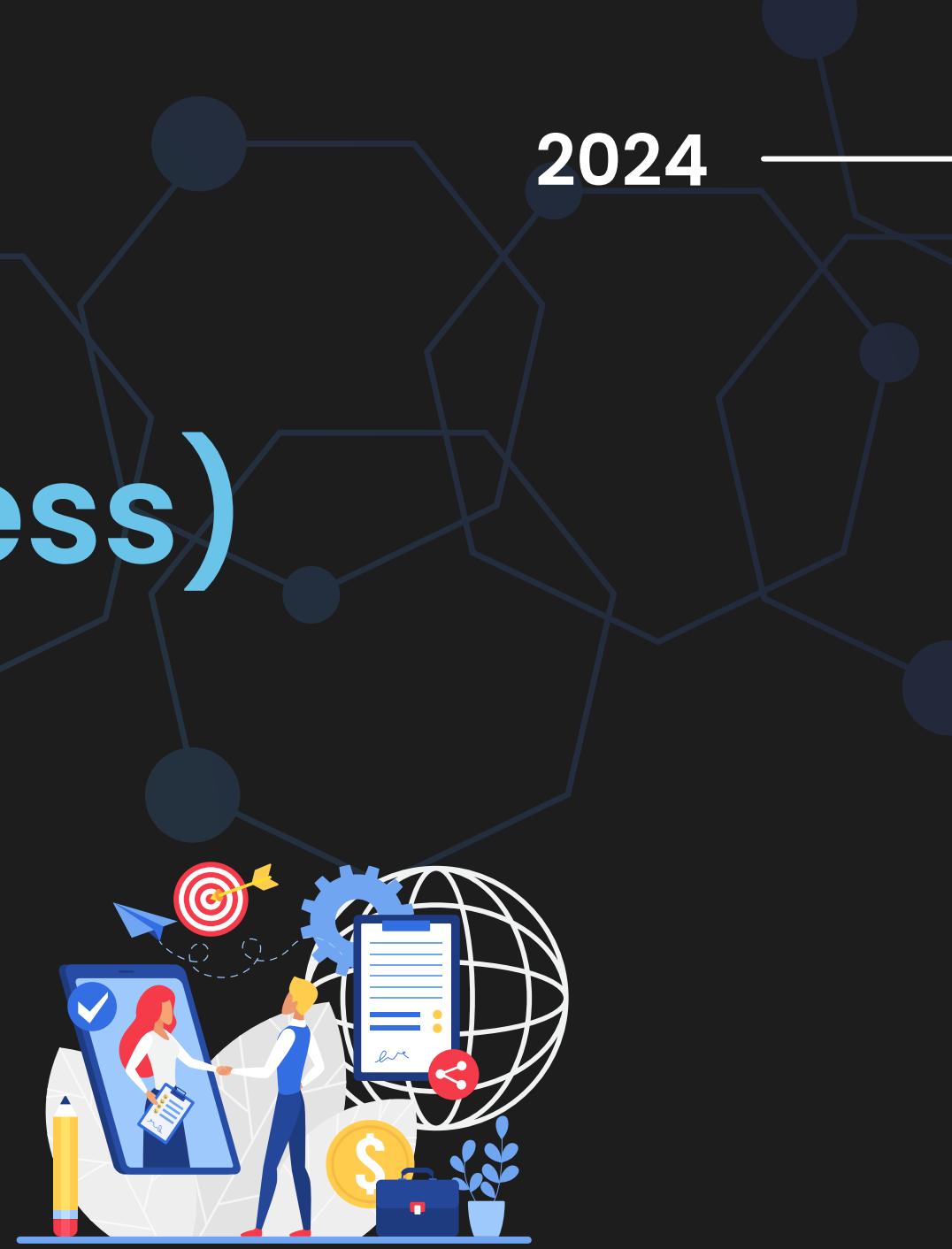
**Small Business  
Owners**

Protecting credit card data and implementing data security standards at point-of-sale registers is cybersecurity.

2024

# Cyber Security (Online Business)

"Cybersecurity involves securing servers that are regularly accessed by untrusted outsiders."



Online Business



Cyber Security

# Cyber Security (Service providers)

Protecting numerous data centers that house servers hosting virtual servers for different organizations is an essential aspect of cybersecurity.



Service Provider

# Cyber Security (the government)

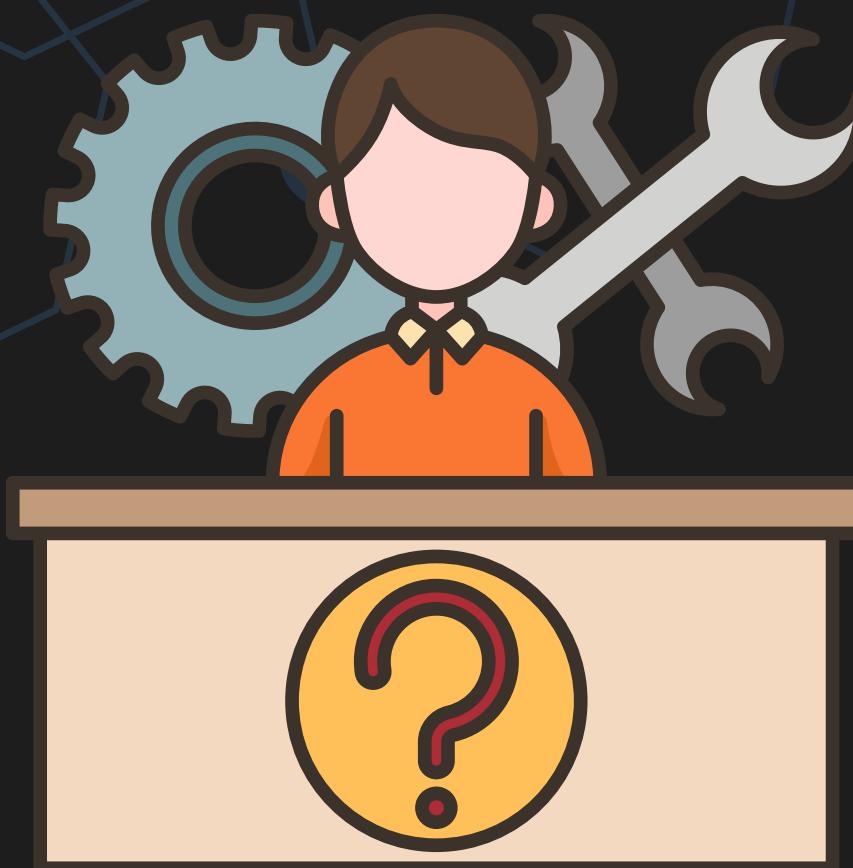
Establishing different data classifications with unique laws, policies, procedures, and technologies is a key aspect of cybersecurity.



Government

# Cyber Security (For us)

**Cybersecurity** is a branch of information security that protects electronic data and systems that store and process it. In contrast, information security encompasses the security of all forms of data.  
(for example, securing a paper file and a filing cabinet)



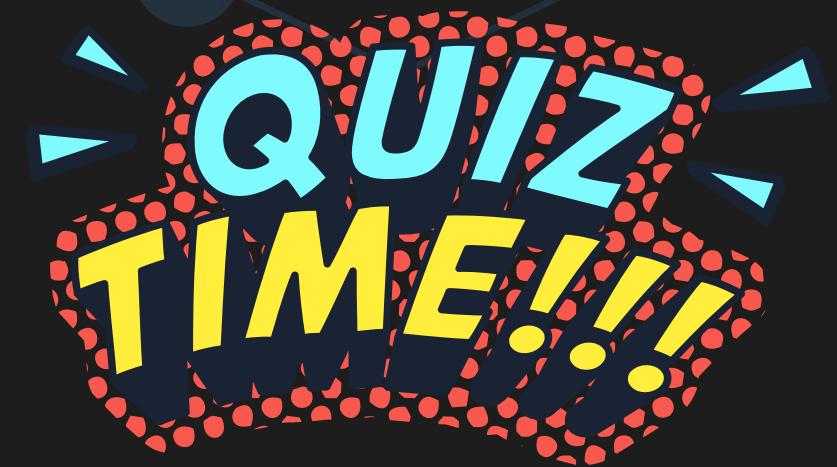
Technical person



# Class Activity

Which of the following is the primary focus of cybersecurity for individuals?

- A. Protecting credit card transactions
- B. Maintaining data classifications
- C. Control over personal data and device functionality**
- D. Protecting virtual servers



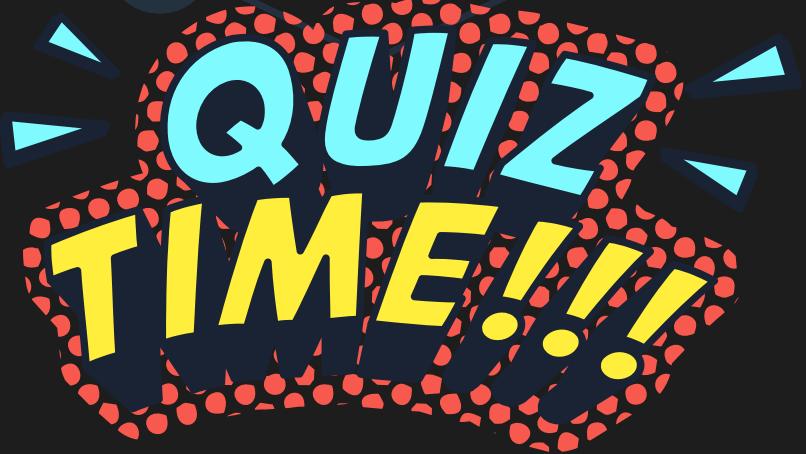


# Class Activity

A small business owner is concerned about cybersecurity.

Their top priority should be:

- A. Establishing server security for online interactions
- B. Complying with data security standards at point-of-sale
- C. Setting up data centers and virtual servers
- D. Classifying data according to government regulations

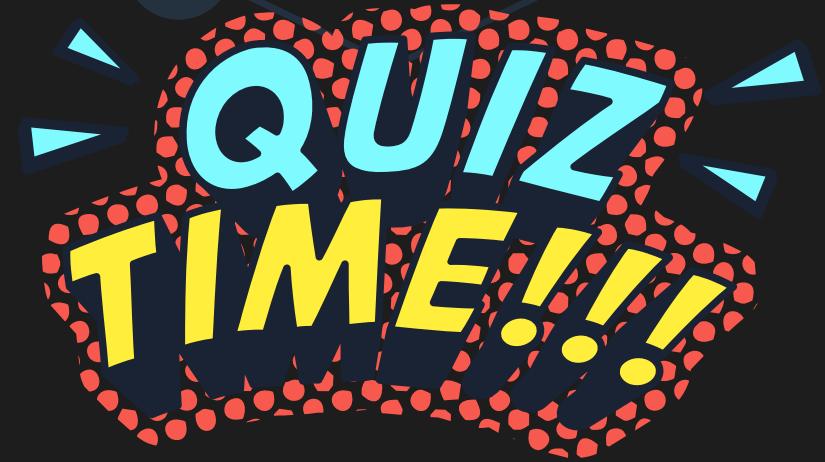




# Class Activity

**What is likely the biggest cybersecurity concern for firms  
conducting online business?**

- A. Preventing malware on personal devices
- B. Securing servers accessed by the public**
- C. Protecting credit card information
- D. Authorizing individual user access to data

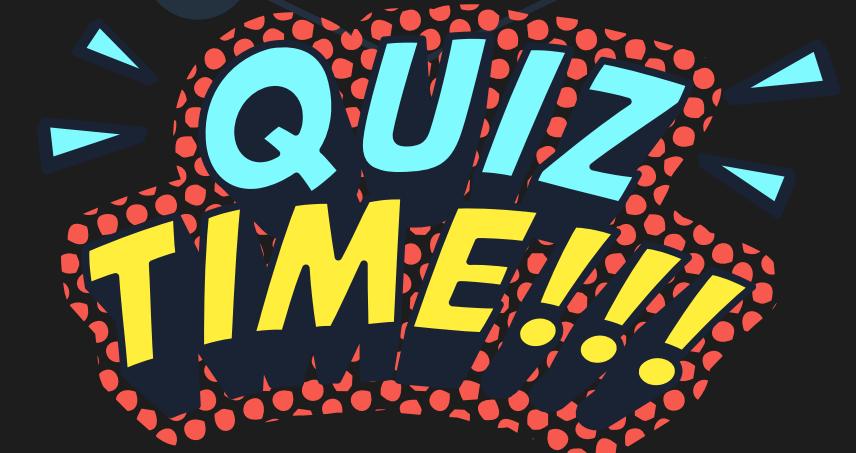




# Class Activity

Shared service providers primarily need to focus their cybersecurity efforts on:

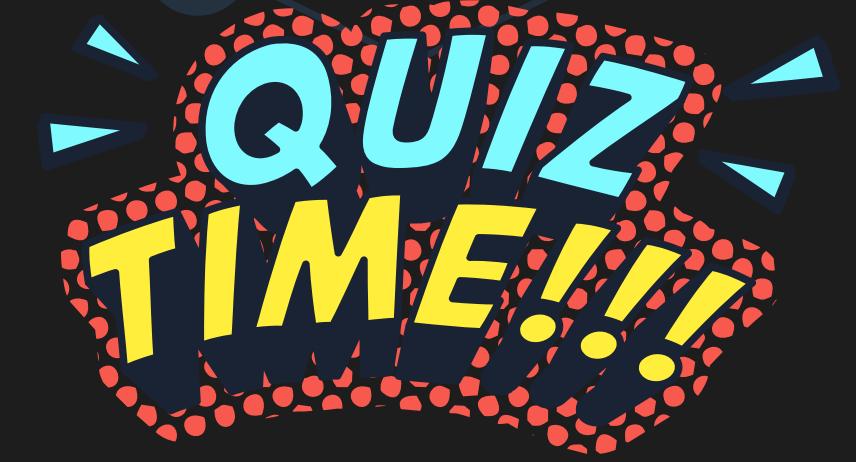
- A. Classifying and labeling government data
- B. Implementing secure point-of-sale systems
- C. Safeguarding large-scale data centers**
- D. Monitoring individual user behavior



# Class Activity

The government's approach to cybersecurity often involves

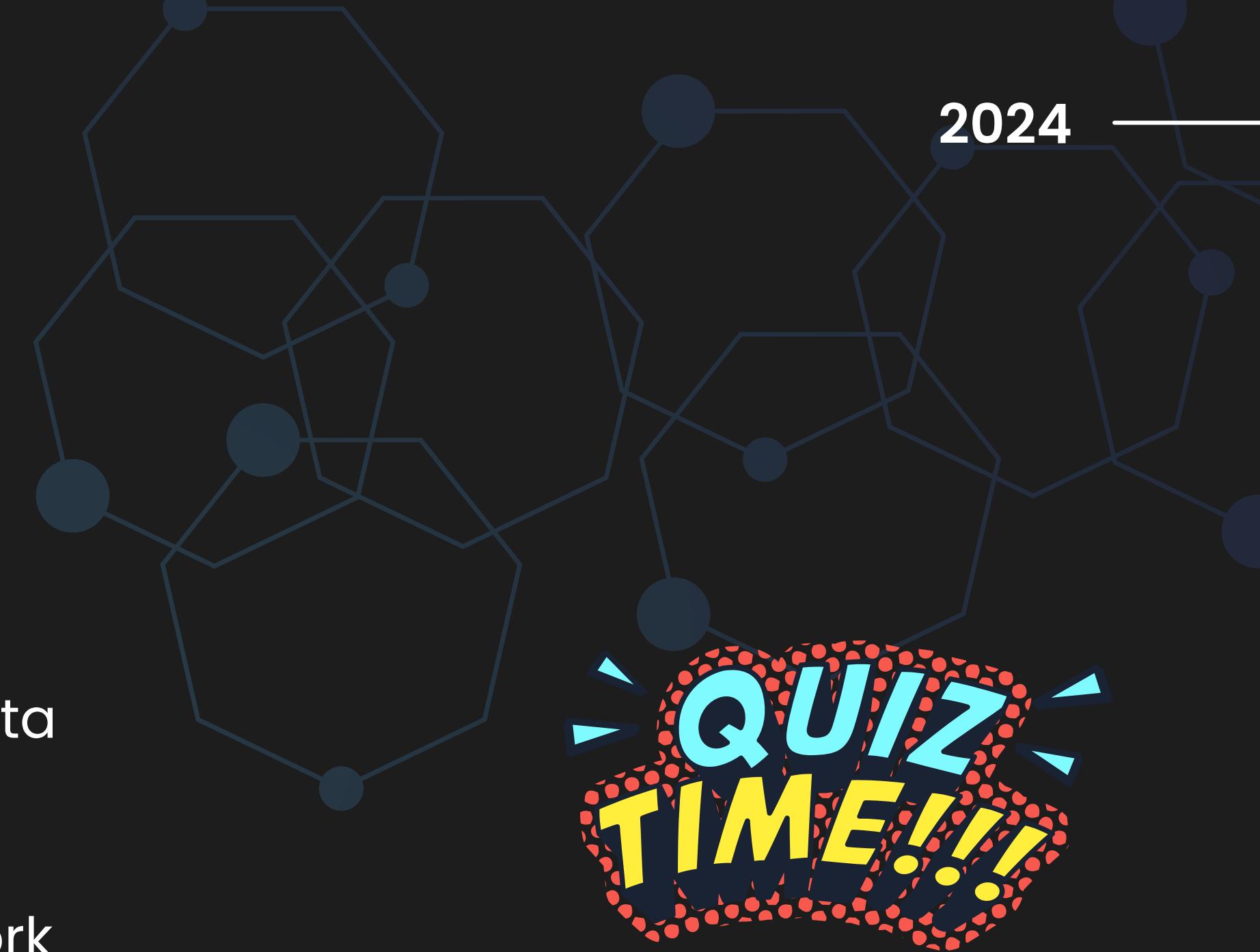
- A. Limiting malware infections on citizen devices
- B. Setting up secure connections for the public
- C** Creating data categories with specific security protocols
- D. Maintaining point-of-sale hardware at businesses



# Class Activity

Protecting personal data means ensuring:

- A Only authorized people can access the data
- B. Devices are classified by security levels
- C. No malware exists anywhere on the network
- D. Servers are secure from any intrusion





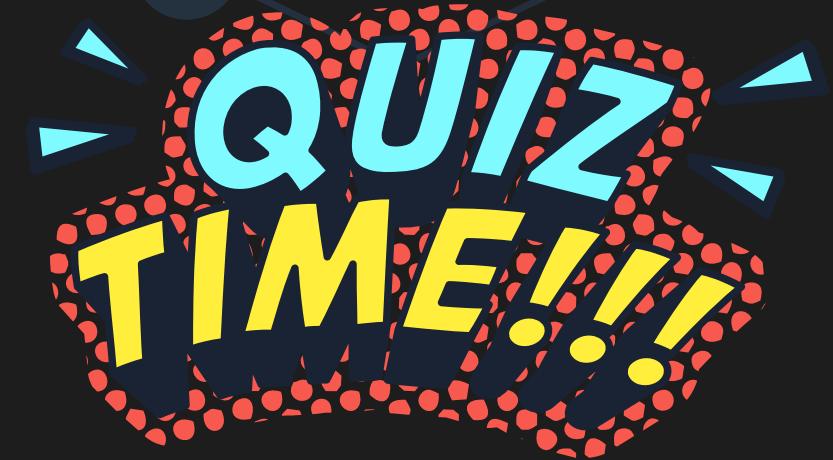
# Class Activity

**Small business owners concerned with cybersecurity should**

**NOT focus on:**

- A. Point of sale security
- B. Government standards
- C. Protecting customer data
- D. Setting up virtual servers

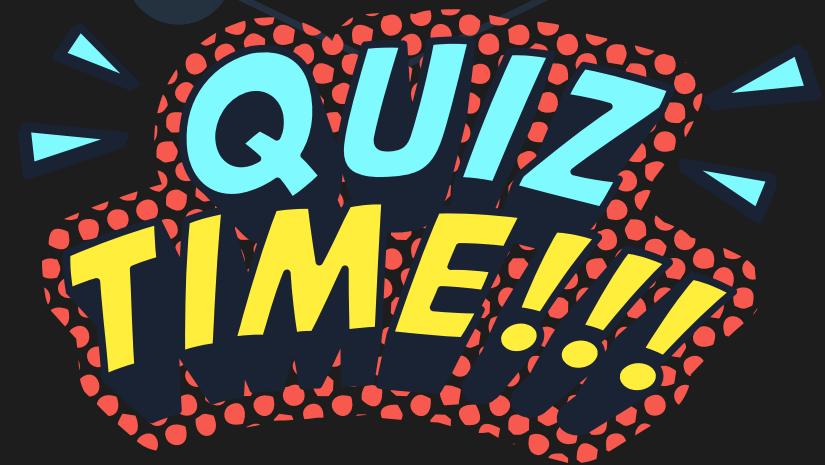
**D**



# Class Activity

The main difference in cybersecurity focus between small businesses and individuals is:

- A. Individuals don't need to worry about malware
- B. Small businesses have customer data to protect
- C. Individuals focus on device functionality
- D. Small businesses don't have data classification concerns

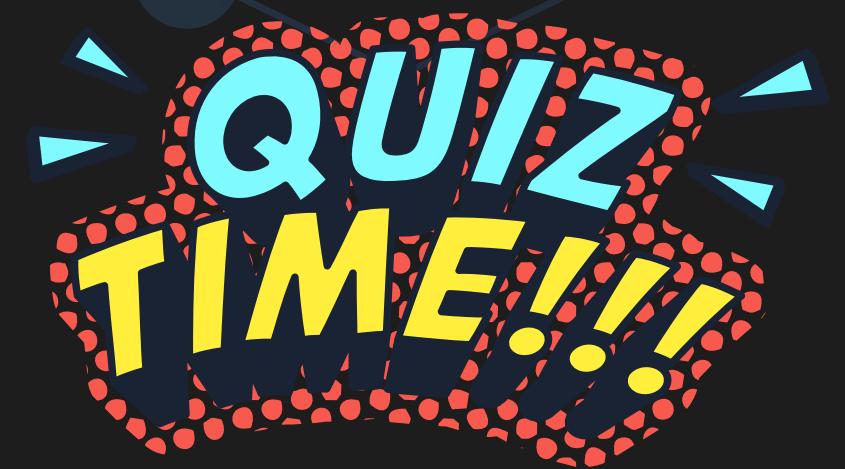




# Class Activity

Which group is LEAST likely to be concerned with point-of-sale security?

- A. Shared service providers
- B. Firms conducting online business
- C. The government
- D. Small business owners



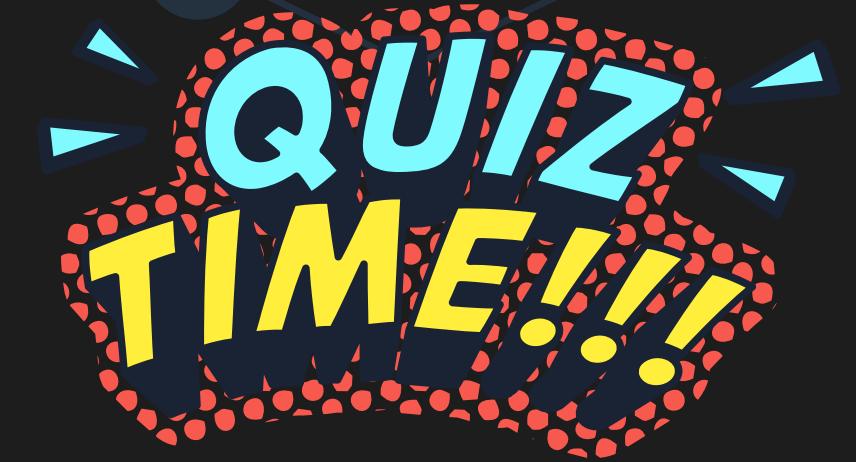


# Class Activity

A cybersecurity threat that applies to ALL the groups

mentioned in the examples is:

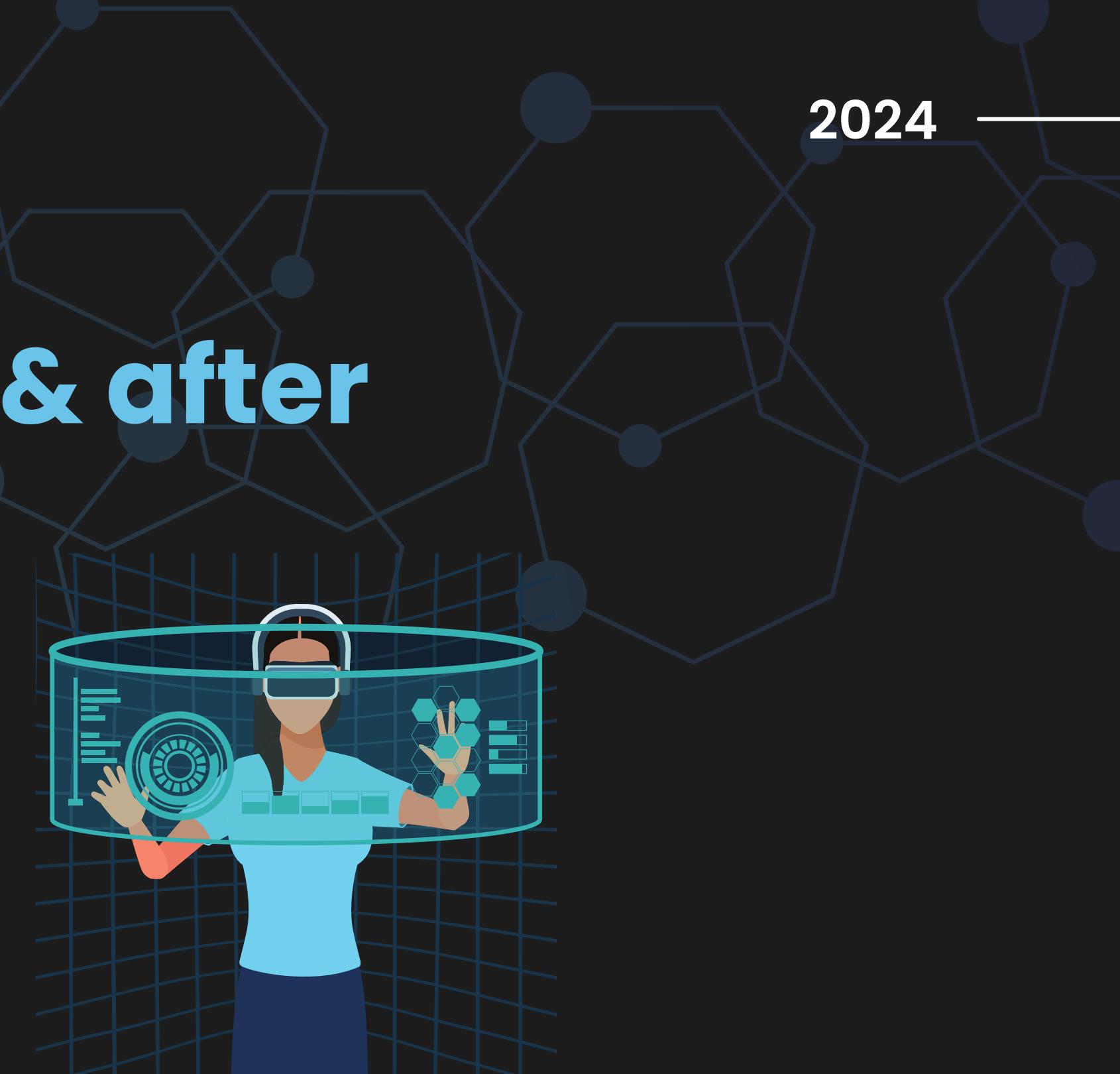
- O** A. Unauthorized data access
- B. Physical theft of point-of-sale devices
- C. Government changes in data classification
- D. Public server failures



# Cybersecurity before & after



remain the same



Keep Changing

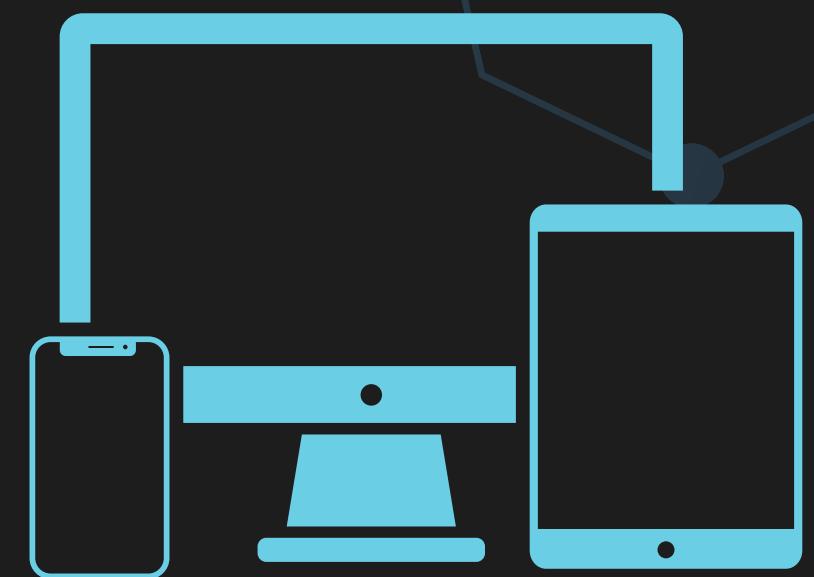
# Technology Change



Data



Internet



Smart Devices



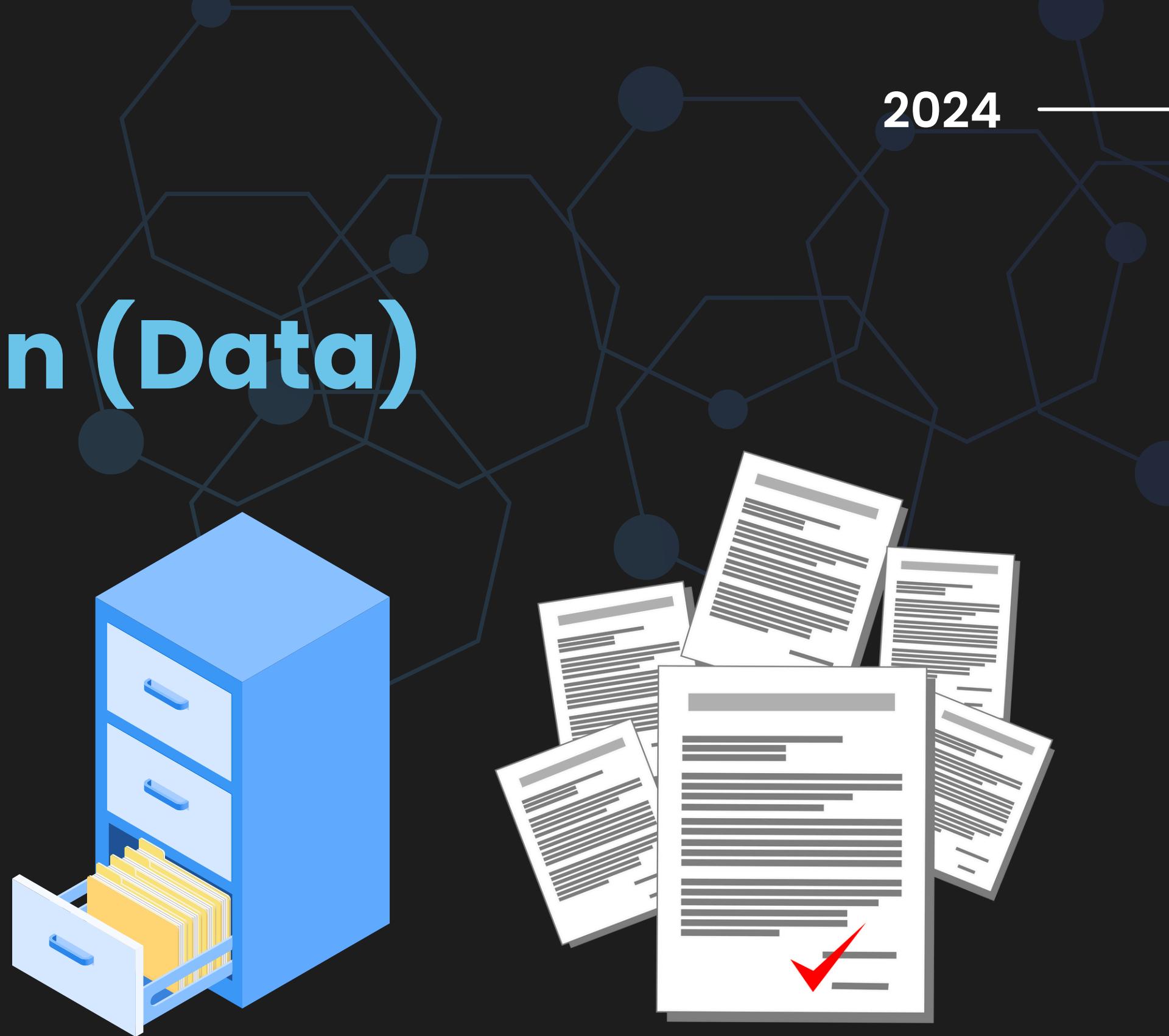
Cryptocurrency

2024

# Cyber Security Then (Data)

**Physical security was key**

- **locked cabinets,**
- **controlled access,**
- **limited hours.**



# Cyber Security Now (Data)

**Digital storage requires complex**

- **Always-on security.**
- **Authentication,**
- **Authorization,**
- **Secure data delivery,**
- **Constant protection against attacks is essential.**



# Cyber Security (Internet)

- The Internet's evolution expanded attack surfaces, allowing hackers to disrupt infrastructure, influence elections, and steal vast sums.
- Cybercrime wasn't very lucrative pre-internet. The growth of online banking and commerce changed that, causing a surge in malicious activity.





# Cyber Security (Smart Devices)

**Smart devices and global sourcing pose new cybersecurity challenges.**

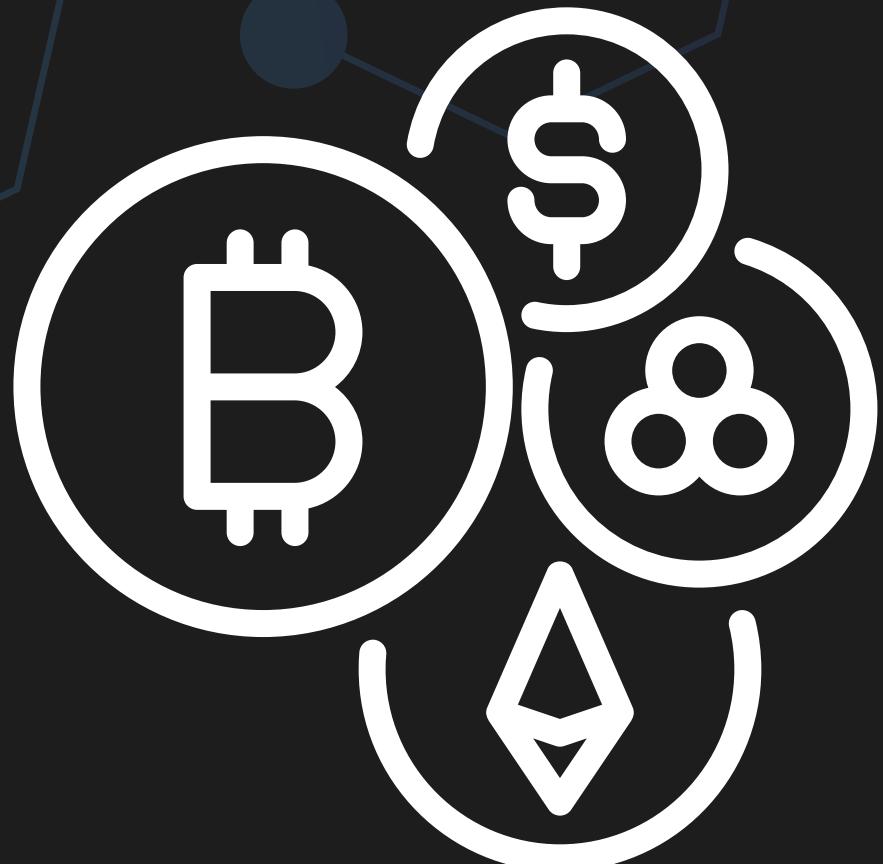
- The IoT explosion has replaced secure machines with hackable ones.
- Cheap IoT devices from unknown overseas suppliers introduce security flaws into homes and businesses via the global supply chain.



# Cyber Security (Cryptocurrency)

**Cybercriminals increasingly use cryptocurrency to fund their operations and evade detection.**

- Ease of transferring stolen funds



# Cyber Security (Social Shifts)

**Societal changes regarding information sharing and online connectivity dramatically expand the toolkit for cybercriminals.**

- Oversharing on Social Media
- Demand for Accessibility
- Digital Shift
- Global Interconnectivity



**Social Change**



# Cyber Security (Economy Model shift)

**Globalization and outsourcing significantly expand the attack**

**surface, requiring new cybersecurity strategies such as:**

- Protecting data in transit across borders
- Preventing backdoors in code or hardware sourced internationally
- Targeting less secure suppliers as a way to infiltrate main targets



**Globalization**

# The goal of Cyber Security

Understanding the principles of **Confidentiality**, **Integrity**, and **Availability** serves as the foundation for a cybersecurity strategy. This knowledge is beneficial in comprehending hackers' objectives and attack methods.



# Why do we care about Cybersecurity?

- Privacy risks
- Financial risks
- Professional risks
- Business risks
- Personal risks
- Physical danger risks



