CYBER SECURITY AND ONLINE SAFETY

www.rcomcomputerservices.com

INTRODUCTION

- *Technology is integrated into every part of our lives*
- *Our dependence on digital systems makes security essential.*
- *Cyber threats continue to grow in number and sophistication*
- *Everyone - individuals and organizations - must adopt strong cyber hygiene to comply with regulatory requirements*
- *Online safety is no longer optional; it's a necessity*

COLORADO CYBER SECURITY LAWS

That pertain to the Electrical Industry

- Colorado Privacy Act (“CPA”) (C.R.S. Title 6, Article 1.3)
- Colorado Information Security Law (C.R.S. § 6-1-713.5)
- Colorado Data Breach Notification Law (C.R.S. § 6-1-716)
- Colorado Document Disposal Law (C.R.S. § 6-1-713)
- Protections for Consumer Data Privacy (HB18-1128)

RCOM COMPUTER SERVICE

WHY CYBERSECURITY MATTERS

- You are required by law to provide cyber security protection for sensitive data that you collect on customers, vendors and employees
- Protects sensitive data (financial, personal, business)
- Prevents financial loss, identity theft, and reputational damage
- Ensures business continuity and operational resilience
- Cybercrime is a multi-trillion-dollar global industry
- Human error accounts for over 80% of breaches

TYPES OF CYBERSECURITY THREATS

RCOM COMPUTER SERVICES

- **Distributed Denial of Service (DDoS) attacks**: Compromised IoT devices are used to overwhelm a target network with traffic, causing it to become unavailable.

- **Malware and Ransomware:** Malicious software can be used to infect devices, steal data, or hold them hostage for ransom.

- **Man-in-the-Middle Attacks:** An attacker secretly intercepts and possibly alters the communication between two parties without their knowledge.

- **Credential Theft:** Attackers use brute force or other methods to guess weak passwords, leading to unauthorized access.

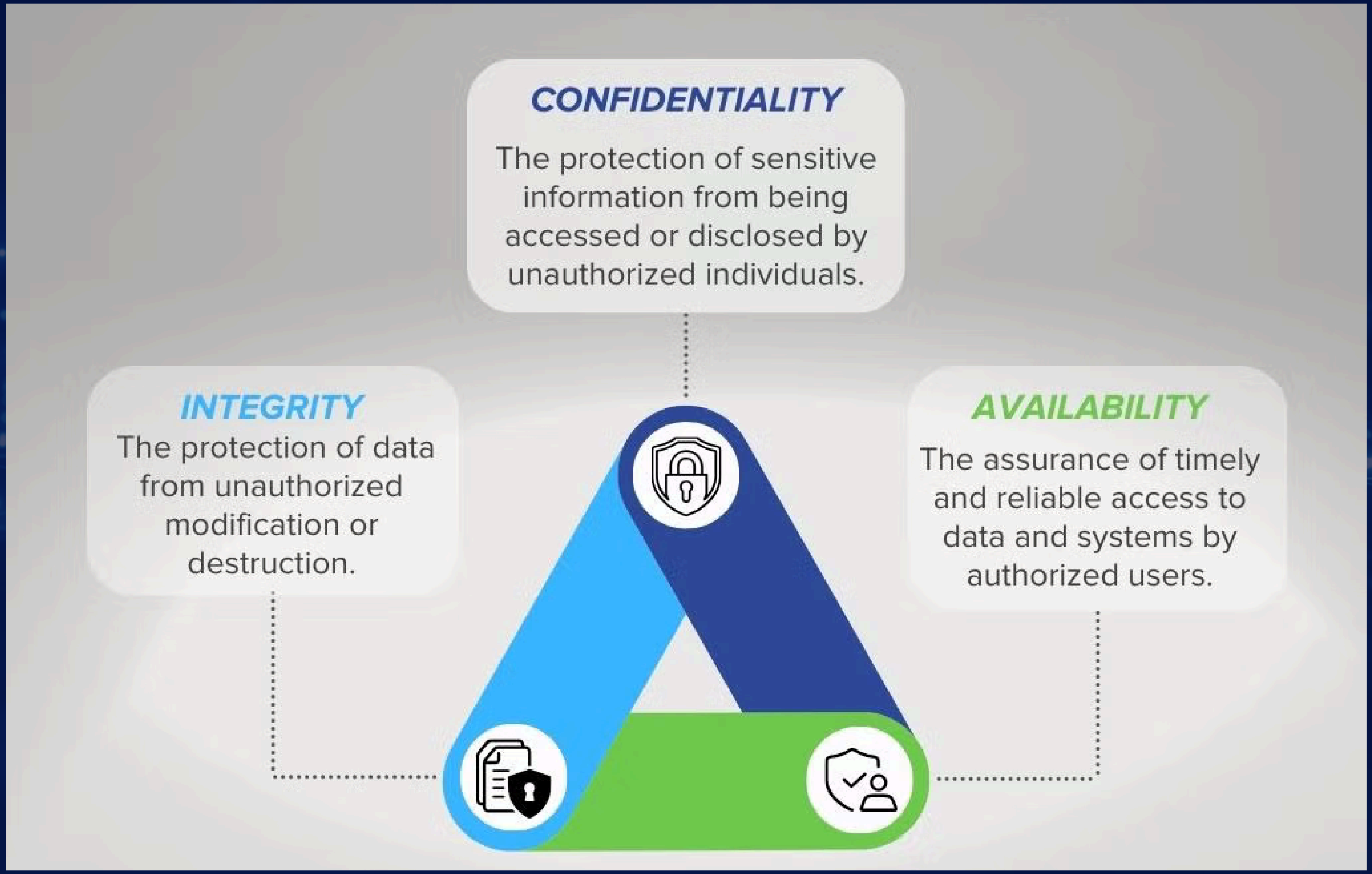
- **Physical Tampering:** This involves physically accessing a device to steal its data or gain control, a risk for devices placed in public areas.

- **Zero-Day Attacks:** These attacks exploit previously unknown vulnerabilities before the manufacturer has a chance to release a patch.

- **Eavesdropping and Data Injection:** Hackers monitor communications to steal sensitive information or inject malicious commands into poorly protected systems.

KEY PRINCIPLES

The **CIA triad** is a fundamental concept in information security and is essential in maintaining the confidentiality, integrity, and availability of sensitive information.



CONFIDENTIALITY

The protection of sensitive information from being accessed or disclosed by unauthorized individuals.

INTEGRITY

The protection of data from unauthorized modification or destruction.

AVAILABILITY

The assurance of timely and reliable access to data and systems by authorized users.

RCOM COMPUTER SERVICES

COMMON CYBERSECURITY VULNERABILITIES

- Weak or reused passwords
- Unpatched software and outdated systems
- Misconfigured networks or cloud services
- Social engineering susceptibility
- Lack of employee training
- Missing or weak MFA (Multi Factor Authentication)
- Public Wi-Fi usage risks
- Poor data backup practices

Most cyber incidents are preventable with good hygiene.

Cybersecurity Frameworks

- NIST Cybersecurity Framework
- ISO/IEC 27001 & 27002
- CIS Controls (Center for Internet Security)
- COBIT (Control Objectives for IT)
- SOC 2 / HIPAA / PCI DSS compliance frameworks

Frameworks provide structure, policies, and best practices.

Tools & Technologies

- Antivirus & Endpoint Detection (EDR/XDR)
- Firewalls & Next-Gen Firewalls
- Multi-Factor Authentication (MFA)
- Password Managers
- VPNs & Zero-Trust Access
- Data Encryption
- SIEM systems (Security Information & Event Management)
- Automated patching & monitoring tools

No single tool provides complete protection; layered security is critical.

RCOM COMPUTER SERVICES

CYBERSECURITY FOR INDIVIDUALS

- Use strong, unique passwords + a password manager
- Enable MFA (Multi Factor Authentication) everywhere
- Never click unknown links or attachments
- Keep software updated
- Use secure Wi-Fi & VPN
- Back up important data
- Limit what you share online
- Verify website security (https://)

Emerging Cybersecurity Trends

- AI-driven cyberattacks & AI-based defenses
- Deepfakes used for fraud & impersonation
- Quantum computing impact on encryption
- IoT & smart device vulnerabilities
- Supply-chain cyberattacks
- Zero-trust architecture adoption
- Cloud security becoming top priority

Conclusion

“The best defense is preparation.”

- Cybersecurity is everyone’s responsibility
- You are required by law to protect the data you collect and the penalties for not doing so can close your doors
- You can’t afford to not be protected
- The majority of breaches are preventable
- Staying secure requires awareness, training, and strong tools
- Small actions make a big difference
- Purchase cyber security insurance for your protection

1982

Providing Expert IT Services
Since 1982

RCOM COMPUTER SERVICES
4868 Innovation Drive
Unit 500
Fort Collins, CO 80525
(970) 460-0484

www.rcomcomputerservices.com

Offices in Texas and Colorado

THANK YOU

Scan this QR Code for a copy of the Presentation