



## Cybersecurity Awareness Month: Staying Informed and Protected

by [Sydney Hillard](#), BSS Staff

Business System Solutions is your IT Service Partner who provides peace of mind through guidance, education, and responsive support. Serving communities in Indiana and Tennessee.

### Caretakers of Your Productivity.

Then Jesus said, "Come to me, all of you who are weary and carry heavy burdens, and I will give you rest."

Matthew 11:28

Cybersecurity is the practice of protecting technology and sensitive information from digital attacks that aim to access, alter, destroy, or expose data. Each October, Cybersecurity Awareness Month serves as a reminder for individuals and organizations to stay vigilant and take the necessary steps to protect themselves against cyber threats.

### Types of Cybersecurity

Cybersecurity encompasses several areas including AI security, critical infrastructure security, network security, endpoint security, application security, cloud security, information security, and identity security.

**AI security** helps safeguard artificial intelligence systems from cyberthreats and malicious use. Cybercriminals may use AI software to create malicious codes, create convincing phishing scams, and attempt to expose confidential information.

**Critical infrastructure security** protects the systems, networks, and facilities that are vital to a nation's society, economy, and public health.

**Network security** prevents unauthorized access to computer networks, helping to detect and stop cyberattacks and security breaches.

**Endpoint security** protects devices, such as desktops, laptops, smartphones, and servers against cyberattacks and unauthorized access.

**Application security** helps secure software applications by identifying vulnerabilities that could lead to unauthorized access, modification, or misuse.

**Cloud security** helps safeguard an organization's data, applications, and other resources that are stored or accessed through cloud-based services.

**Information security** protects sensitive information, including digital files, paper documents, and physical media from unauthorized access, use, or alteration.

**Identity security** protects digital identities and the systems used to manage them, including verification codes, authentication apps, and biometric authentication such as fingerprint or facial recognition.

Together, these areas provide multiple layers of security to protect systems, data, and users from potential cyber threats.

## The Most Common Cyberthreats

Some of the most common cyberthreats include malware, ransomware, phishing attacks, insider threats, AI attacks, and distributed denial-of-service (DDoS).

**Malware**, also known as malicious software, is software or code that is meant to harm a computer system or its users.

**Ransomware** is a type of malware that locks or encrypts a victim's sensitive data, making it inaccessible, and even demanding a ransom to restore access. In 2026, 39% of breached organizations reported being affected by ransomware, compared to 34% in 2025 and 24% in 2023.

**Phishing attacks** are fraudulent emails, texts, or voice messages that trick users into sharing sensitive information, downloading malware, or transferring funds to hackers or fraudulent accounts. For example, a phishing email may appear to come from a trusted source and contain links or attachments that look legitimate.

**Insider threats** occur when authorized users, such as employees, contractors, or business partners intentionally or accidentally misuse their access, potentially putting an organization's system or information at risk.

**AI attacks** involve the malicious use or manipulation of artificial intelligence to create harmful content, expose sensitive information, or spread false information.

**Distributed denial-of-service (DDoS) attacks** occur when cybercriminals attempt to make a website, online service, or other resource inaccessible by overwhelming it with traffic.

Recognizing common cyberthreats and how they occur can help individuals and organizations reduce their risk and respond more effectively.

## Common Cybersecurity Misconceptions

There are multiple misconceptions surrounding cybersecurity, including

**Strong passwords are sufficient protection.** Even though strong passwords are important, they only offer one layer of protection. Adding measures like multi-factor authentication and regular security updates can help strengthen the overall security.

**Most cybersecurity risks are well known.** As technology constantly evolves, so do cyber threats and vulnerabilities. New threats can easily go unnoticed, making it important to stay aware of potential risks.

**All cyberattack entry points or pathways are identifiable and managed.** Cybercriminals consistently find new entry points to access systems and data. While known vulnerabilities can be addressed, new or previously unidentified vulnerabilities still create opportunities for attacks.

**Some industries are safe from risks.** Although the type of attack varies, every industry can be affected by cyberattacks.

**Cybercriminals don't attack small businesses.** Small businesses are not exempt from cyberattacks. In 2025, 80% of small businesses experienced at least one cyberattack.

## Best Practices To Help Prevent Cybercrime

Everyone can play a part in helping prevent cybercrime. One helpful approach is the 3 Ds of cybersecurity: Deter, Detect, and Delay. This method focuses on discouraging threats, identifying them early, and slowing their progress.

**Deter:** Discourage the attack or threat from occurring by implementing various security measures.

**Detect:** Identify and verify threats early to provide greater response times and limit their potential impact.

**Delay:** Slow an attack with layers of security that make it more difficult for an attacker to succeed.

When a threat or attack cannot be identified and prevented, the 3 Rs of cybersecurity: Respond, Report, and Recover, become equally important. These steps can help mitigate the impact of an incident and support recovery.

In addition to these approaches, daily cybersecurity practices can also help reduce the risks:

- Use strong, unique passwords.
- Enable multifactor authentication (MFA) and a secure password manager.
- Avoid and report phishing scams.
- Regularly update software and devices.

The 3 Ds, 3 Rs, and daily cybersecurity practices can help strengthen overall security and better protect important information.

~~~

Cybersecurity Awareness Month reminds us that staying informed and taking proactive steps can make a difference in creating a more secure environment. For further assistance, the BSS team is here to help. Contact our Indiana office at 765-742-3440, our Tennessee office at 615-819-0600, or email us at [support@bssconsulting.com](mailto:support@bssconsulting.com). □

## The BSS ADVISOR

[info@bssconsulting.com](mailto:info@bssconsulting.com)

**North-Central Indiana Office**  
1211 Cumberland Avenue  
West Lafayette, IN 47906  
(765) 742-3440

**Middle Tennessee Office**  
1026 West College Street  
Murfreesboro, TN 37129  
(615) 819-0600

Channel Partners.  
**MSP501**  
2025 WINNER

# Client Appreciation Lunches

## Indiana



## Tennessee



We are so grateful for our incredible clients and team!