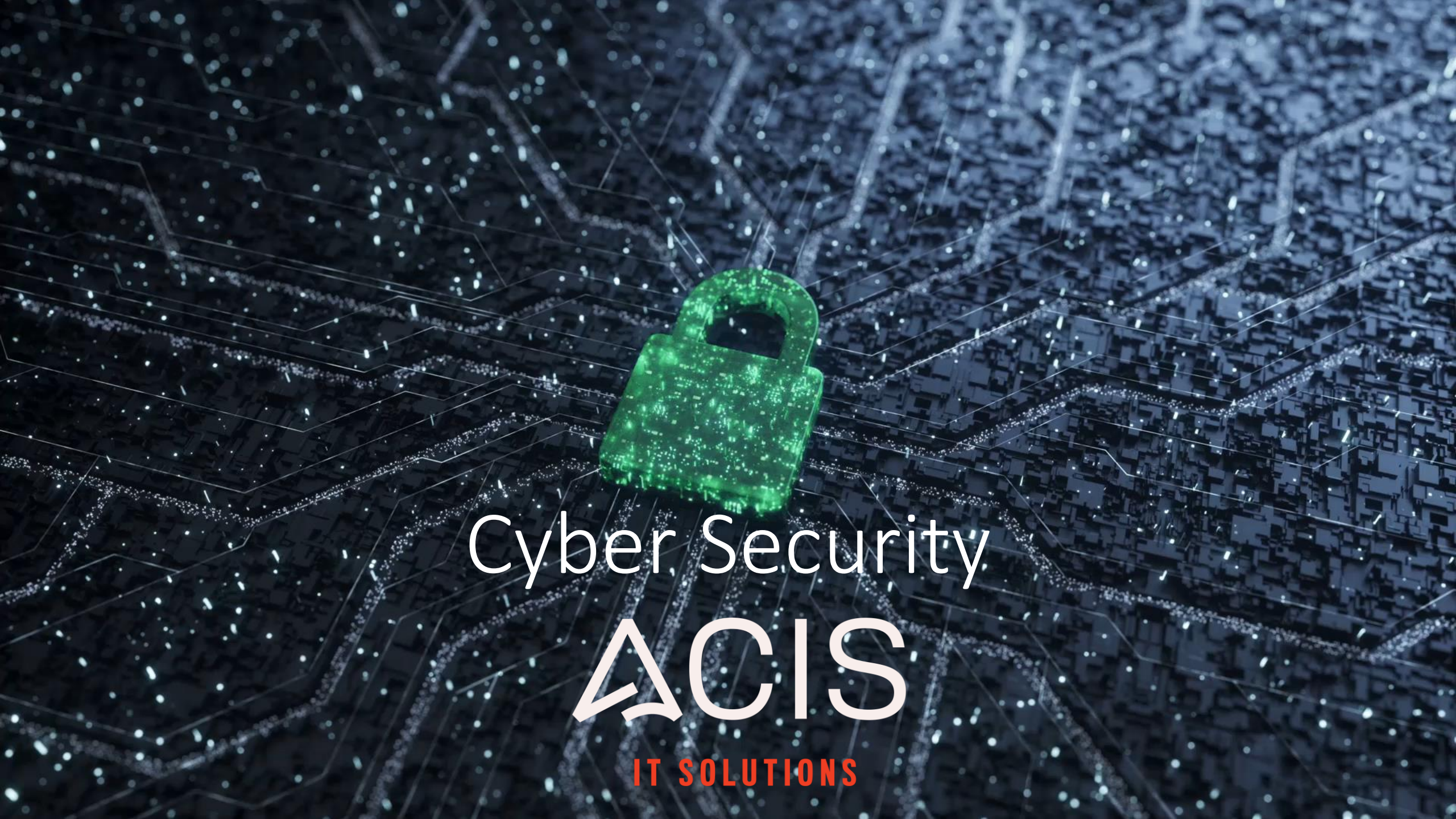
Cyber Security
ACIS
IT SOLUTIONS

What is Cyber Security?

Cyber Security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Categories of Cyber Security

- Network security – The practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- Application security – Focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- Information security – Protects the integrity and privacy of data, both in storage and in transit.
- Operational security – Includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- Disaster recovery and business continuity – Define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.
- End-user education – Addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

A few interesting statistics

- 93% – The number of breaches that begin with phishing emails
- 98% – The amount of organizations that have malicious emails in users inbox’s
- 57% – The percentage of companies using MFA in 2019
- $4,000,000 – The average cost of a breach/ransomware attack

Email is the #1 target for all breach attempts

What is a data breach?

- An incident in which information is stolen or taken from the owner without his/her knowledge or permission.
- If the stolen information includes the names, and medical or financial records of individual persons, the owner of such information – in most states – has obligations under the law to address the breach and notify the impacted individuals.
- Example – Target notified people of a breach of credit card accounts and passwords that happened in 2013.

How is email used in breaches?

- Social Engineering - the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
- Fake Accountant/CFO scams
- Phishing emails
- Compromised email accounts

Examples of Social Engineering

- Phishing: tactics include deceptive emails, websites, and text messages to steal information.
- Spear Phishing: email is used to carry out targeted attacks against individuals or businesses.
- Baiting: an online and physical social engineering attack that promises the victim a reward.
- Malware: victims are tricked into believing that malware is installed on their computer and that if they pay, the malware will be removed.
- Pretexting: uses false identity to trick victims into giving up information.
- Quid Pro Quo: relies on an exchange of information or service to convince the victim to act.
- Tailgating: relies on human trust to give the criminal physical access to a secure building or area.
- Vishing: urgent voice mails convince victims they need to act quickly to protect themselves from arrest or other risk.
- Water-Holing: an advanced social engineering attack that infects both a website and its visitors with malware.

Fake Accountant/CFO scams

- Sometimes come from actual email, but is usually a spoofed email account
- Request payment while spoofing an accountant or CFO’s email.
- Usually an ACH request to a bank that is unknown or different.

Always double check when emailed about sending money, especially if they say they are unavailable and not to contact them.

Phishing emails

- Often look legitimate from a known company asking you to verify, reset or authenticate your account.
- Sometimes threating legal action or doxing due to inappropriate content found on the computer, recorded video during use, etc.
- Sometimes list a previous, possibly current password that was obtained through a large password breach in the past.

Compromised email accounts

- Often, the user of the compromised account has no idea they have been compromised.
- People on your contact list may get spam emails
- Fake accountant/CFO scams can be done from the account
- Usually has a rule setup in the account to forward messages to the RSS Feeds folder in Outlook so the user does not see them.
- Messages are deleted as they get replied to from RSS Feeds and Sent Items.

How to identify a spoofed or fake email

- Check the actual email address in the from field. If the email is not shown in brackets behind the name, click on the name to show the email address. If it looks odd or isn't what it should be, it's likely a spoof.
- Poor grammar or spelling is a tell-tale sign due to most being from non-English-speaking countries.
- The signature is off in some way, missing an image, plain text or not like it usually is from that person.
- The language used is not normal for the person emailing you.

How can you protect your email?

- Turn on Multi-Factor Authentication for email
- Requires multiple ways to authenticate
  - something you know, passwords, secret questions, etc
  - Something you have: Token, badge, or application
  - Something you are: Fingerprint, retina, behavior
- Even if password compromised, multi-factor prevents access
- Cyber insurance is requiring MFA

Ransomware

- A form of malware designed to encrypt files on a device or network devices, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.
- Emails are used to infect devices and networks through links or files that run the ransomware code. Often fake invoice or shipping notice files are used. Always check the link before you click on it by hovering over the link to see the full address. You can also right click and copy to paste into another field to see where it is taking you. Pay attention to the domain name. If in doubt, don't click on it and contact your IT Administrator.
- Some emails can run the ransomware code simply by opening the email. To avoid this, use your preview pane for emails. All major modern email clients have disabled the ability to run code in preview. Word files preview in email can still run code in some cases. If in doubt, do not open anything and contact your IT Administrator.

How can you protect your environment?

- Through established Cyber Security guidelines and procedures.
- The National Institute of Standards and Technology, NIST, has created a Cyber Security Framework of best practices for your IT safety.
- Network security best practices can help harden your network.
- Have a written disaster recovery plan
- Patch Management
- Anti-Virus Endpoint Protection and Endpoint Detection and Response
- Understand the level of security you really need.

Network Security

- Use a next generation firewall appliance to protect your network. A home style router may be good for your home but is not robust enough to protect your school or business network.
- Separate networks using a virtual LAN so that access is limited for certain groups such as a student and teacher network.
- Separate your guest WiFi from your internal network to not allow guests to affect your internal network.
- Use Single Sign-On, SSO, authentication through your firewall to filter content based on user credentials.

Disaster Recovery Plan

- The ability to quickly handle incidents can reduce downtime and minimize both financial and reputational damages. Furthermore, DRPs allow organizations to ensure they meet all compliance requirements, while also providing a clear roadmap to recovery and contain guidelines as to who handles what in a disaster.

Patch Management

- Ensure security updates are done in a timely manner on devices on the network.
- Updating firewall firmware on a regular basis.
- Updating all network equipment, including switches, access points, network attached storage devices, etc.

Anti-Virus

- Having a centrally managed Endpoint Protection Program and Endpoint Detection and Response can lower your risk of malware infection and response times
- Updating your anti-virus software on a regular basis helps with malware detection.
- Zero-day algorithms, or heuristics scan software behavior for malicious activity to detect viruses that are not yet known.

What level of security do you really need?

- When you follow all the guidelines and perform maximum security, accessing data can become inconvenient.
- Too much security can cause stress in employees and lead to lower security and bad practices such as:
  - Failing to log off or lock a computer when leaving the area.
  - Writing down passwords on notes kept on the desk.
  - Using less secure, easy to guess passwords due to constant password change requests.
  - Copying secure data to an external device for easier access.
- Know your environment and adjust for an appropriate level of security.
- Be concise with your security policies and why they exist.

Questions?

Thank you for taking the time to attend this presentation.