Security Best Practices

Cybersecurity begins with you! Yes, you!

INTERNET SECURITY

At this point in technological history, every organization should protect internal resources with a firewall. Ensure that your firewall can block based on geolocation and that it can do stateful inspection and sandboxing. Ensure the firewall has comprehensive logging capabilities.

NETWORK PROTECTION

Deploy Intrusion Prevention Systems to monitor, detect and block malicious activity within your network. Implement it so that it is not only monitoring ingress and egress but also traffic between subnets to detect lateral movement.

LEGACY TECHNOLOGY

Companies should identify their o unsupported technology and dependencies and develop replacement system and device lifecycle plans. Legacy software and applications increase the organization's cyber risk and vulnerability.

- **Use Endpoint Detection and Response Solutions (EDR)**
  EDR monitors user behavioral analytics, endpoint connections, and process execution. It also analyses data to identify anomalies and malicious activity and records information about it, empowering security teams to address incidents. Anti-virus alone isn't enough anymore.

- **Back Up Data**
  Back up critical data and systems. Have multiple copies of your backups. Regularly test backups to ensure their validity.

- **Least Privilege**
  It's the principle of assigning only the minimum permissions necessary in order to carry out job duties and business functions.

- **Implement Multi-factor Authentication (MFA)**
  MFA stops 99.9% of fraudulant login attemps on your accounts.

- **Cyber Awareness Training**
  Train your people to know and understand the risks of technology and common attacks like phishing, social engineering, and Business Email Compromise (BEC)

- **Keep software up-to-date**
  Patching systems and applications reduces the attack surface and cyber risk and improves performance.

- **Administrative Privilege**
  Tightly control who has administrative privileges within your organization.

- **Device Monitoring and Control**
  Understand what devices are on your network and their risk potential. This can be done manually or by implementing a solution like Network Access Control (NAC).

- **System Configuration**
  Ensure that systems are securely configured before placing them into production. Consider adopting the CIS Controls and establish baseline configurations.

NEBRASKA
Good Life. Great Vision.
OFFICE OF THE CIO

BUILDING A CYBER STRONG NEBRASKA