BEFORE THE BREACH (BUSINESS)

For farms and ag businesses who work with an IT provider or have larger scale IT infrastructure, such as servers for their operation.

Checklist

Vulnerability and Configuration Management

- ☐ Update software, operating systems, applications and firmware on IT network assets in a timely manner.
- ☐ Use a centralized patch management system.
- ☐ Replace end-of-life software; i.e., software that is no longer supported by the vendor.

Secure Access

- ☐ Require strong, complex and unique passphrases for each user.
- ☐ Enforce Multi-Factor Authentication (MFA) for all users, without exception.
- ☐ Enforce MFA on all VPN connections. If MFA is unavailable, require employees engaging in remote work to use strong passwords.
- ☐ Regularly review, validate or remove privileged accounts (annually at a minimum).

Protective Controls and Architecture

- ☐ Properly configure and secure internet-facing network devices, disable unused or unnecessary network ports and protocols, encrypt network traffic, and disable unused network services and devices.
  - ☐ Harden commonly exploited enterprise network services, including Link-Local Multicast Name Resolution (LLMNR) protocol, Remote Desktop Protocol (RDP), Common Internet File System (CIFS), Active Directory and OpenLDAP.
- ☐ Segment networks to limit or block lateral movement by controlling access to applications, devices, and databases.
- ☐ Continuously monitor the attack surface and investigate abnormal activity that may indicate lateral movement of a threat actor or malware.
- ☐ Use security tools such as Endpoint Detection and Response (EDR), and Security Information and Event Management (SIEM) tools.
- ☐ Monitor the environment for potentially unwanted programs, or implement application control.
- ☐ Ensure you back up critical systems and test backups regularly.

Employee Training

- ☐ Annually provide security awareness training to employees.
- ☐ Provide a method to allow employees to report suspicious behavior.