Cybersecurity for Agriculture

Dr. Taylor Reynolds
treyn@mit.edu
Cybersecurity: Hooded hacker?

Always need a “Hooded hacker”

Pictures with “binary code” is an added bonus
Cybersecurity: Scary big numbers?
This is not one of those presentations
Cyber attacks are indeed a big and complex problem
MIT SCRAM project - Measuring cyber risk

6  Maintenance, Monitoring, and Analysis of Audit Logs
12 Boundary Defense
1  Inventory and Control of Hardware Assets
8  Malware Defenses
16 Account Monitoring and Control
20 Penetration Tests and Red Team Exercises
18 Application Software Security
17 Implement a Security Awareness and Training Program
14 Controlled Access Based on the Need to Know
4  Controlled Use of Administrative Privileges
9  Limitation and Control of Network Ports, Protocols, and Services
5  Secure Configurations for Hardware and Software
13 Data Protection
3  Continuous Vulnerability Management
7  Email and Web Browser Protections
10 Data Recovery Capabilities
2  Inventory and Control of Software Assets
11 Secure Configuration for Network Devices
15 Wireless Access Control
19 Incident Response and Management

Sum of losses in USD '000
Security needs differ by the size of the firm

- **Large** (250+)

- **Medium** (50-249)
  - **Small** (10-50)
  - **Micro** (<10)

My day job

This presentation
Agriculture has always used cutting-edge technology

- Smart farming
- Sensors & control systems
- IoT
- Robotics
- Drones
- Precision agriculture
Key recommendations for micro, small and medium enterprises
Key goals

1. Take steps to keep attackers out

2. Don’t let them get away with much if they do make it in

3. Build in resilience to recover from attacks quickly
1. Steps to keep attackers out
Turn on two-factor authentication (2FA)

Your accounts should have two-factor authentication required for logins. That means anyone accessing the account needs the password + a code that is texted to their phone or created on a rotating basis by an authenticator app.
Use good password hygiene & password managers

Make applications that do password management available to employees (e.g., LastPass, KeePass) and teach them to use strong and unique passwords for each of their accounts and logins.

https://xkcd.com/936/
Teach employees about phishing/malware

The most common attack vector is getting employees to click on links in phishing emails.

Reducing these dangerous clicks that infect a computer and then propagate across the network are critical to keeping attackers out.
Effectively apply software updates & patches

Firms should make sure that they have a plan in place to apply software updates and patches to their systems and machines quickly and efficiently.

Unpatched systems leave security holes open.
2. If they get in, they can’t get much
Only systems that need it get Internet access

One of the best ways to protect critical systems is to keep them disconnected from the Internet.

This is called “air gapping” because it puts physical distance between the connected parts of the network and critical/valuable systems.
Create a separate network for IoT/sensors/controls

Assume that hackers will be able to get into your sensor network and IoT devices.

Keep critical business systems and sensitive data on a separate network and never connect the two.
3. Be able to recover quickly
Perform regular backups

Ransomware is where hackers lock your data and require payment to release it (or not). It is currently the most common cyber attack we see.

Regular & frequent backups are your best defense and use the 3-2-1 rule:

- 3 copies
- 2 media (cloud, hard drive, tape)
- 1 located offsite
Conclusion

Cybersecurity is a challenging problem, but these simple steps can reduce your exposure significantly
Thank you