Nutrien™
Feeding the Future™

Importance of Cybersecurity within Agribusiness

Agenda

1 Introduction

2 Cyber Terminology

3 Cyber Safety and Trends

4 Global State of Cybersecurity

5 Smart Agriculture and Cyber Risk

6 Operational Technology (OT) and Cyber

8 Key Takeaways

Introduction

Legal Guidance: Nutrien Ltd. and its affiliates do not provide information security advice. This material has been prepared for informational purposes only, and is not intended to provide, and should not be relied on for any information security or other advice. You should consult or engage your own information security experts.

Cyber Terminology

1	Malware	Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
2	Phishing	The fraudulent practice of sending malicious emails in order to induce individuals to reveal personal information.
3	Internet of Things (IoT)	the interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data.
4	Ransomware	A type of malicious software designed to block access to a computer system until a sum of money is paid.
6	IT	Information technology (IT) is the development, management, and application of computer equipment, networks, software, and systems. IT is crucial to modern business operations because it enables people and machines to communicate and exchange information.
7	OT	Operational technology (OT) uses hardware and software to manage industrial equipment and systems. OT controls high-tech specialist systems, like those found in the energy, industrial, manufacturing, oil and gas, robotics, telecommunications, waste control, and water control industries.
8	Patching	A patch is a set of changes to a computer program, or its supporting data designed to update, fix, or improve it
9	State Sponsored Actor	Motivated by military, economic, or political interests, typically employing malicious cyber campaigns to gain access to sensitive assets for competitive advantage

Cyber Safety

Phishing Awareness

When fraudulent messages attempt to trick you into giving up information or payment.

Safe Web Browsing

Ensuring you travel to known good websites and avoid malicious sites is key.

Password Management

Passphrases > Passwords where applicable. Learn how to securely store all your passwords.

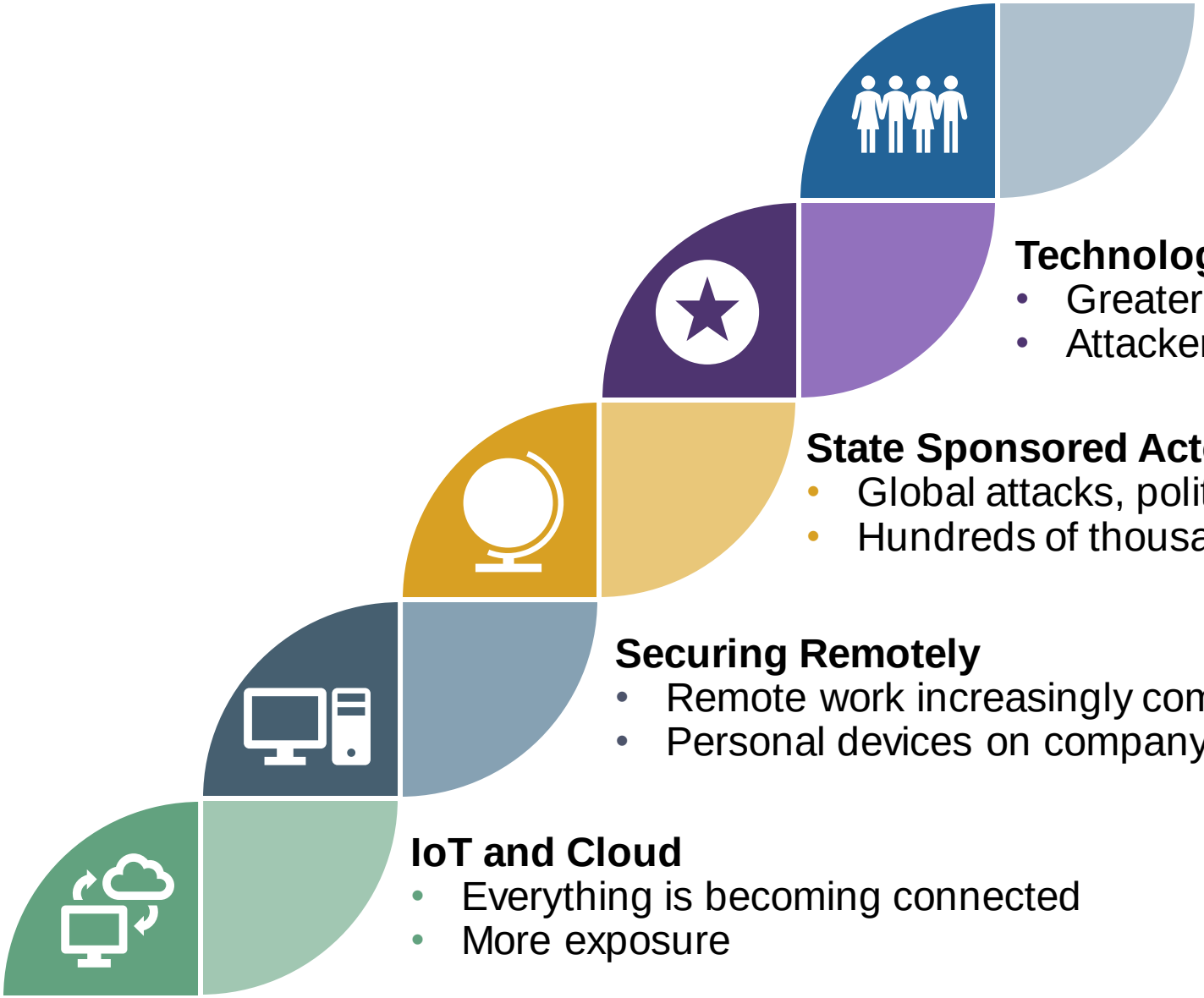
Social Engineering

Threats can come in more than just emails, be wary of suspicious text messages, phone calls etc.

Multi-Factor Authentication

MFA is key to securing accounts wherever it is possible to enable.

Cybersecurity Trends



Security Awareness
- Everyone is a target
- Ensuring a cyber-secure work force is key

Technology Race
- Greater reliance on technology
- Attackers are using new tech as well

State Sponsored Actors
- Global attacks, politically motivated
- Hundreds of thousands of these attacks

Securing Remotely
- Remote work increasingly common
- Personal devices on company networks

IoT and Cloud
- Everything is becoming connected
- More exposure

Global State of Cybersecurity

Agriculture a Growing Threat Target – Why attack us?

Global operations in some of the most targeted countries

Heavy reliance on connections and third party business within supply chains

Targets by state sponsored groups, part of China Five Year Plan

Attackers do their research! Strong years and earnings in ag put us in attackers' crosshairs.

As the Agriculture industry shifts more towards internet enabled technologies this increases the risk of cyber incidents occurring.

More reliance on the internet means more targets to attack and more potential points of access and compromise.

Important Timely Events

CYBER NEWS

Wednesday, April 20th, 2022

Vol 13-15

FBI WARNS OF 'TIMED' RANSOMWARE ATTACKS ON AGRICULTURE SECTOR

Farming and agriculture seen as a lucrative target where victims could be more willing to pay a ransom for a decryption key because of the time-sensitive nature of the industry.

Cyber News

CYBER NEWS

Monday, May 9th, 2022

Vol 13-16

AGCO RANSOMWARE ATTACK DISRUPTS TRACTOR SALES DURING U.S. PLANTING SEASON

Cyber News

CYBER NEWS

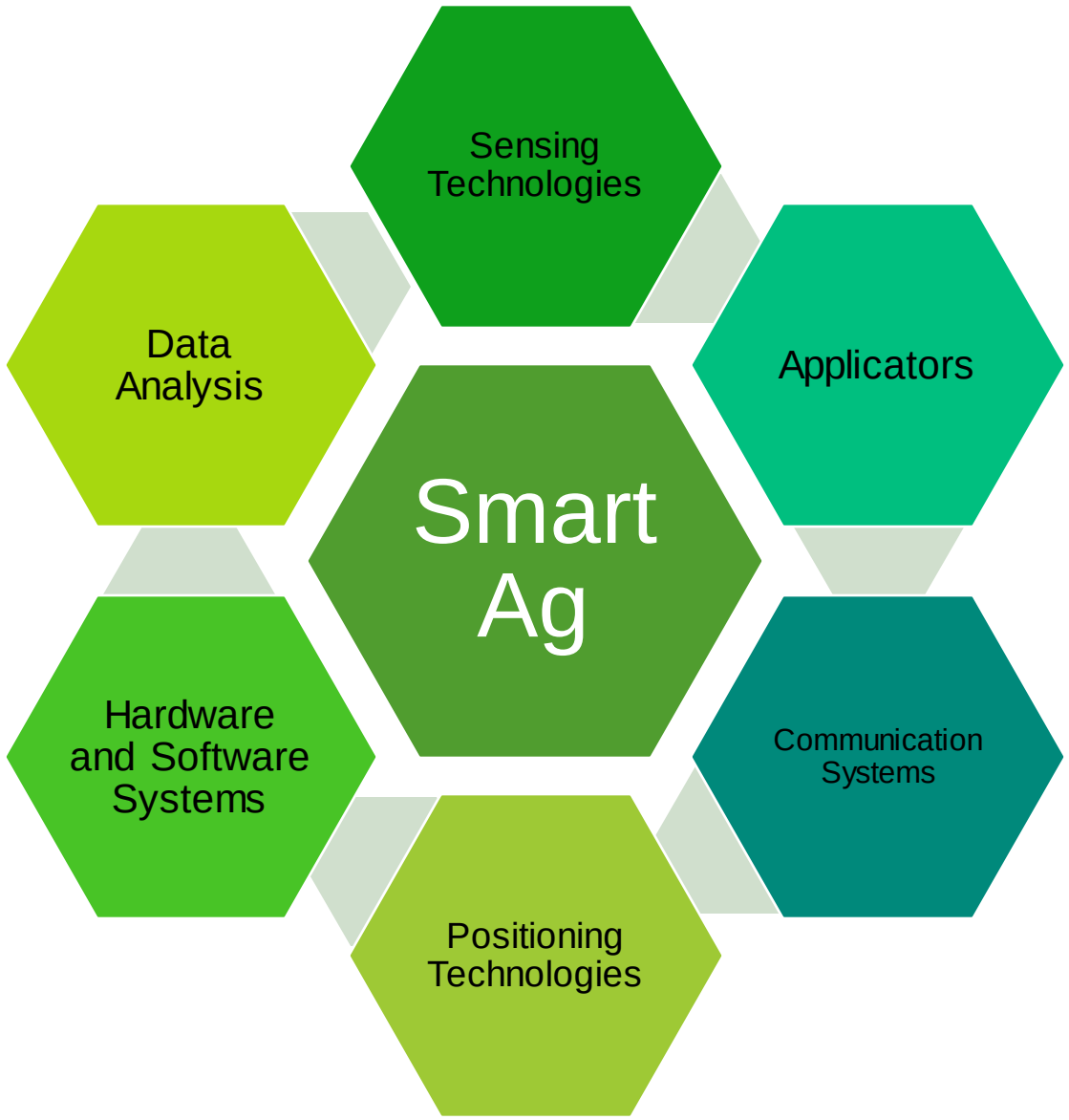
Tuesday, October 11th, 2022

Vol 13-16

PRESIDENT BIDEN SIGNS NSM-16 TO STRENGTHEN U.S. FOOD SAFETY, SECURITY; HIGHLIGHTS CLIMATE CHANGE, CYBERSECURITY

Cyber News

Smart Agriculture + Cyber Risk



IoT
As more devices are there is more opportunity for risk

Limited Patching
These systems often have limited patching or are neglected

Speed of Change
Adopting new tech needs to be done at a pace security can be ensured

Considerations for Protecting Key Networks

	IT	ICS/OT
Business Priority	Confidentiality	Safety, Availability
Major Focus	Data Integrity	Preventing Injuries and Production Downtime
Protection Targets	Windows Computers/Servers	Industrial Devices
Environmental Conditions	Controlled Environments – Air Conditioned, Stable	Harsh Environments – Extreme Temp, Vibrations

Attacks on ICS Systems can lead to real world impacts

Florida Water Treatment Plant

Attacker changed the chemical mix to extremely dangerous levels. Could have caused severe sickness and/or death in the community.

Middle East Oil Refinery

Rare and dangerous new form of malware (Triton) targets industrial safety control systems that protect human life.

Consolidated Grain & Barge Co.

Cyber criminals infected systems and rendered many facilities inoperable, forcing a system-wide shut down.

Colonial Pipelines

Colonial Pipelines suffered a ransomware attack to their payment systems. They shut off their pipeline in response and operations did not restore for 5 days

Key Takeaways

- Everyone is a target, from organizations, to personal accounts, attackers want it all
- There is no one stop shop that fixes all security risks, different technology needs to be secured differently
- Cyber attacks come in many forms targeting many kinds of systems; we might be most familiar with phishing emails but that is not all we need to be aware of

Thank you for listening