2024 Security Report

Prime Pack Beef:
Risk Assessment

BCYB 640 Final Project:
Mya Zylberberg

Today's Agenda

01 **Company Overview**
Who we are

02 **Security Profile**
Understanding our Tier and current situation

03 **Our Baseline**
Scoring the Essential Cyber Hygiene controls

04 **Cybersecurity Challenges**
Real world and Ours

05 **Impacts from Common Threats**

06 **Target Benchmarks**
Planning Priorities and next step actions

Company Overview

Some Key Features of our organization are:

- Food and Agriculture critical infrastructure

- Mid-size cattle and meat packing company

- Located in upstate New York

- 2,000 employees and growing

- Risk appetite – Moderate

Security Profile

IG2 IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

IG1 IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.
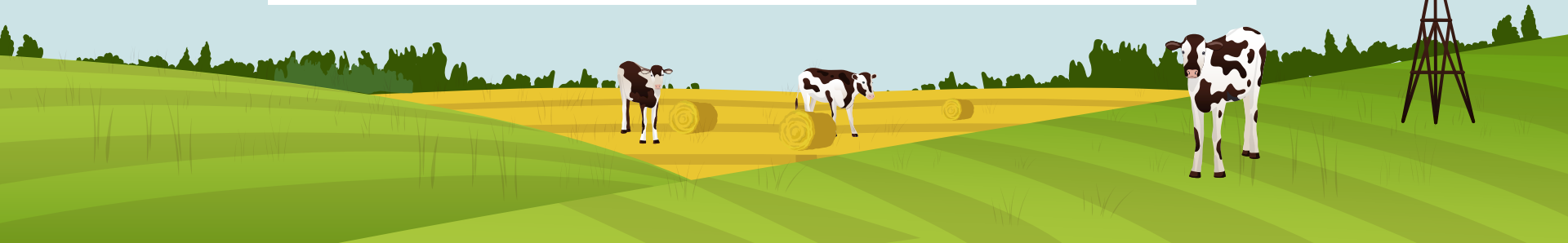
03

Our Baseline

Good, keep it up **Needs attention** **Urgent: fix ASAP!**	**Inventories & Controls:** documented (physical, digital, informational), inspected	**Data protection:** unified classification schema, zero-trust, retention policy, access logs	**Secure Configurations:** restrict personal device use, limit IoT use
Account Management: up -to-date, unique identifiers and passwords	**Access Control Management:** SOP enforcement, required MFA	**Continuous Vulnerability Management:** automate patching/ monitoring, track updates, frequent reviews	**Audit Log Management:** systematically (establish, collect, review, retain)
Email & Web Browser Protections: reliably outsourced	**Malware Defense:** restrict unauthorized devices, enable anti-exploitation features	**Data Recovery:** systematically (establish, collect, review, retain)	**Network Infrastructure (Management, Monitoring & Defense):** reliably outsourced
Servicer Provider Management: 3rd party vetting, contracted, monitored, updated as needed	**Security Awareness & Skills Training:** organization-wide, additional role-based, reporting procedures	**Incidence Response Management:** standardize procedures, reporting system, after action reviews	

04

Cybersecurity-Related Challenges

Real -World Incidents

- JBS Foods Ransomware Assault

- Danish Crown Cyberattack

- Schreiber Foods Ransomware Incident

Our Incident

- Prime Pack Beef Ransomware Incident

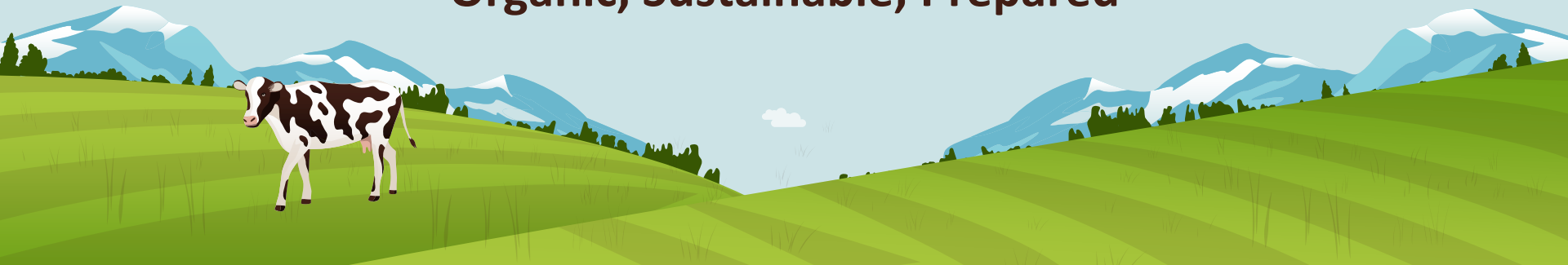# Impacts from Common Threats

- Product Contamination/Quality

- Consumer Trust

- Financial Losses

- Company Reputation

- Lawsuits

Target Benchmarks

1. Network Security

2. Data Encryption

3. Access Controls & Authentication

4. Incident Response Plan (IRP) creation

5. Employee Training & Awareness

Organic, Sustainable, Prepared

Sources

• White House. (2022). National Security Memorandum on Strengthening the Security and Resilience of U.S. Food and Agriculture. Retrieved from https://www.whitehouse.gov

• CISA. (2015). Food and Agriculture Sector-Specific Plan. Retrieved from https://www.cisa.gov

• Bloomberg News. (2021). Danish Crown Meat Processor Hit by Cyberattack. Retrieved from https://www.bloomberg.com

• National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from https://www.nist.gov

• Cybersecurity and Infrastructure Security Agency. (2024). Internet of Things Security for Critical Infrastructure. Retrieved from https://www.cisa.gov

• A guide to Critical Infrastructure Security and Resilience (2019). Retrieved from https://www.cisa.gov/sites/default/files/publications/nipp-ssp-food-ag-2015-508.pdf