



Cyber Threats to Food and Agriculture

15 NOV 2022

Presented by Donald Hester, Cybersecurity Manager

City of Livermore, Cybersecurity Division



“This is an important part of the core mission of the City government which is to keep citizens safe.”

- Mayor Bob Woerner

Initiative Goals:

- Increase public cyber safety
- Cyber-crime prevention
- Promote economic development and innovation
- Community resilience
- Empower an inclusive future

California Commodities

California Provides:

- 1/3 of the United States vegetables
- 2/3 of the United States fruits and nuts
- 36% of US organic production
- 20.8 Billion in agricultures exports (2020)

Wine Specifically:

- 81% of all U.S. wine
- World's 4th leading wine producer
- \$57.6 billion in state economic impact
- 325,000 jobs in California
- \$17.2 billion in state wages

Sources: U.S. Tax and Trade Bureau; BW166; The Gomberg, Fredrikson Report; Global Trade Information Services; and California Dept. of Food & Agriculture; Cal-CSIC.

Key Threat Drivers

- Vintners, Ranchers and Farmers integrate technology into their practices
- Cyber risks increase with the adoption of new technologies



Source: sourcetrace.com

IoT

Internet of Things

- Physical devices connected to the internet
- Sensors
- Robotics (UAV)
- GPS
- Monitors (Crop Monitoring)



Operational Technology

Process Automation

- Industrial control systems (connected)
- Planting, Irrigation, Monitoring
- Sorting
- Fermentation
- Bottling and Packaging



Source: phys.org

Information Technology

Office Operations

- Data
- Financial
 - Invoice, Payments, Banking
- Shipments
- Marketing
- Communication
- Employee Personally Identifiable Information



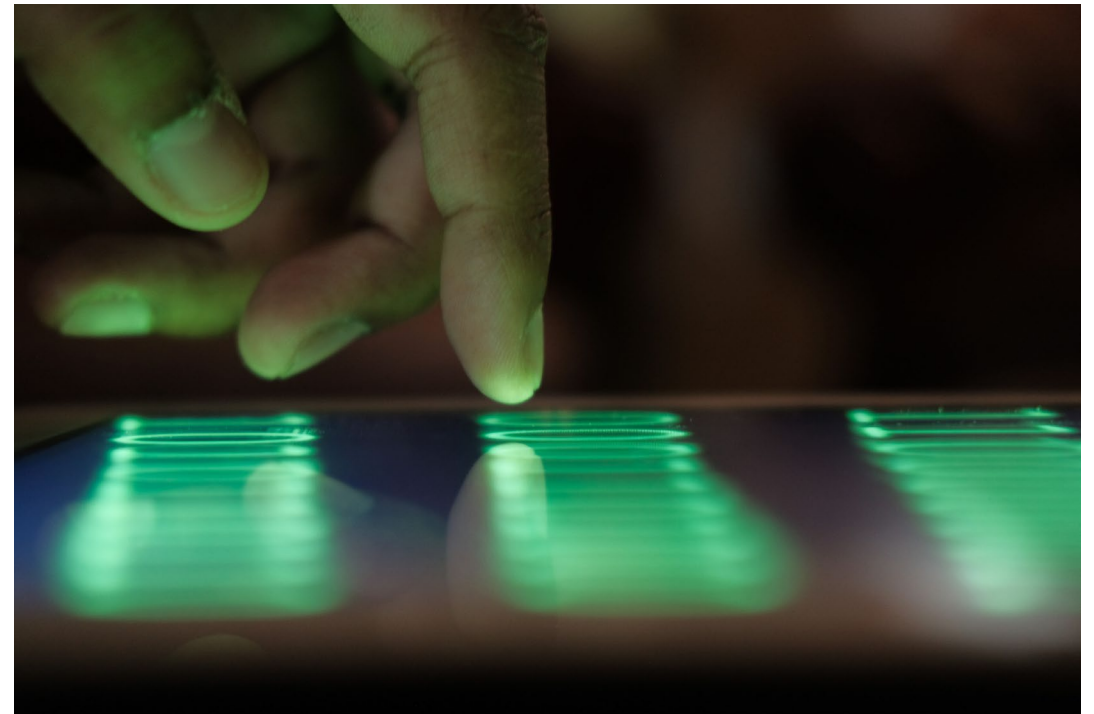
Supply Chain Risks

- Financial loss
 - Colonial Pipeline incident increase fuel and shipping costs
- Disruption or Delay on operations
- Reputational damage
 - A vendors incident reflects on the organization



The Bad Guys

- Cyber Criminals
 - Financial motivated
 - Ransomware & Extortion
- Nation States
 - Economic advantage
 - Disruption & destruction
 - Intellectual property
- Hacktivists
 - Agenda based



JBS Foods Ransomware Attack

- May 30, 2021
- REvil Ransomware Attack
- Stop operations at 13 meat processing plants
- Russian Based
- White House contacted Russia
- Paid \$11M in ransom
- Some suspects were arrested



Source: Getty Images

Types of Attacks on Food and Agriculture

- Ransomware
- Data Breach
- Computer Intrusion
- Malware/Scamware
- Business Email
- Compromise
- Supply Chain



Critical Infrastructure Food and Agriculture Sector

Dependencies particularly with the following sectors:

- Water and Wastewater Systems
- Transportation Systems
- Energy
- Chemical

FOOD AND AGRICULTURE SECTOR

The Food and Agriculture Sector is almost entirely under private ownership and is composed of an estimated 2.1 million farms, 935,000 restaurants, and more than 200,000 registered food manufacturing, processing, and storage facilities. This sector accounts for roughly one-fifth of the nation's economic activity.



The Food and Agriculture Sector has critical dependencies with many sectors, but particularly with the following:

- [Water and Wastewater Systems](#), for clean irrigation and processed water
- [Transportation Systems](#), for movement of products and livestock
- [Energy](#), to power the equipment needed for agriculture production and food processing
- [Chemical](#), for fertilizers and pesticides used in the production of crops

[Expand All Sections](#)

[Sector-Specific Plan](#) +

[Sector Resources](#) -

For resources available to Food and Agriculture Sector partners, visit the [Department of Agriculture](#) and the [Food and Drug Administration](#) websites.

<https://www.cisa.gov/food-and-agriculture-sector>

Cyber Safe Livermore Initiative



- Cybersecurity for Business
- Cybersecurity Education and Career
- Report Cyber Crime
- About Cybersecurity Division
- Cyber Safety App
- Cyber Safety Basics
- Disinformation Stops With You
- Phishing Defenses
- Cybersecurity Career
- Work Cyber Safe at Home
- Passwords
- Data Handling
- Lost Computer
- Removable Media
- Vishing
- Downloads
- Public Wi-Fi

Cyber Safe Livermore Initiative

Cybersecurity Awareness Month and Beyond

Cyber threats and the damage caused by them continue increase an in order for us to push back we need everyone to work together against those cyber threats. Every day in the news we hear new stories of cyber-attacks and there seems to be no end in sight. There is a growing understanding there needs to be public private collaboration at all levels if we want to stem the tide.

"The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy." - President, Joseph R. Biden Jr.

Cyber-crime, if measured, would be the 3rd largest economy in the world with over \$6 trillion in global damages. The impact of cyber breaches is disproportional to individuals and small businesses. Small to medium sized businesses and individuals do not have access to the same resources necessary to protect themselves from cyber criminals, cyber bullies, nation states, or any other cyber bad guys. Many small businesses that become victims of cyber-attacks file for bankruptcy or go out of business.

Impact on Small Businesses

- 30% of small businesses experienced an official breach
- 25% of them filed for bankruptcy
- 10% of them went out of business

Cyber Safe Inclusion

The recent congressional Report from the Cyberspace Solarium Commission noted that cybersecurity is critical to improving digital citizenship. In working to bridge the digital divide cybersecurity is essential, in fact the Global

Print Feedback Share & Bookmark Font Size



- Cybersecurity
- Family Cyber Safety
- Cybersecurity for Business
- Cybersecurity Education and Career
- Report Cyber Crime
- About Cybersecurity Division
- Cyber Safety App
- Cyber Safety Basics
- Disinformation Stops With You
- Phishing Defenses
- Cybersecurity Career
- Work Cyber Safe at Home
- Passwords
- Data Handling
- Lost Computer
- Removable Media
- Vishing
- Downloads
- Public Wi-Fi
- Digital Spring Cleaning

Departments » Administrative Services » Cybersecurity »

Cybersecurity for Business

Print Feedback Share & Bookmark Font Size

Working together to make Livermore cyber safe.

Cybersecurity Resources for Small and Medium Businesses (SMB)

The links on this page take you to other websites not managed by the City of Livermore. The City of Livermore is not responsible for the content of external sites.

General Resources

- [National Cyber Security Alliance: Homepage \(staysafeonline.org\)](#)
- [CyberSecure My Business™ - Stay Safe Online](#)
- [Resources for Business | CISA](#)
- [Resources for Small and Midsize Businesses \(SMB\) | CISA](#)
- [CIS Center for Internet Security \(ciscsecurity.org\)](#)
- [Bad Practices | CISA](#)
- [StopRansomware.gov](#)
- [NIST Computer Security Resource Center | CSRC](#)
- [Cybersecurity Framework | NIST](#)
- [Business Privacy Resources | State of California - Department of Justice - Office of the Attorney General](#)
- [Search Data Security Breaches | State of California - Department of Justice - Office of the Attorney General](#)
- [InfraGard](#)
- [Information Sharing and Analysis Centers](#)

Tech Tips

- [Technology Checklist For Businesses \(Download Tech Tips\)](#)

Alerts and Bulletin

<http://CyberSafe.LivermoreCA.gov>

<https://www.livermoreca.gov/departments/innovation-economic-development>

