



**SinnovaTek**

Leading the Next Wave of Food  
Innovation and Sustainability  
May, 2024



# Leading the Next Wave of Food Innovation

## The SinnovaTek Team





# Food Processing Experts on a Mission

NUTRIENT RETENTION CLEANER LABELS REDUCE WASTE INCREASED SHELF LIFE NATURAL

## Our Mission:

Promote worldwide health and wellness by fostering the delivery of high quality, healthy food through sustainable methods





## Be The Change We Seek



- Certified B Corporations are to business what Fair Trade certification is to coffee or USDA Organic certification is to milk.
- B Corps are for-profit companies certified by the nonprofit B Lab to meet rigorous standards of social and environmental performance, accountability, and transparency.
- Today, there is a growing community of more than 4,000 Certified B Corps from 70+ countries and over 130 industries working together toward 1 unifying goal: to use business as a force for good.
- This global movement now includes 200+ Food & Beverage companies.





# Company Structure



## Equipment

- ▶ SinnovaTek (Parent Company)
  - ▶ Equipment Manufacturing
  - ▶ Technology Development
  - ▶ Services (Formulation, Engineering, Food Safety)



## Ingredients

- ▶ Sinnovita
  - ▶ Ingredient Supplier
  - ▶ Extraction and Complexation Development
  - ▶ Utilizes SinnovaTek Technology and Equipment



FIRSTWAVE

## Manufacturing

- ▶ FirstWave
  - ▶ Precision-Scale Manufacturer
  - ▶ Showroom Floor / Demonstration Site
  - ▶ Utilizes SinnovaTek Technology and Equipment





# Food Processing Ecosystem in NC

Improving Access to Food Manufacturing



R&D, Feasibility  
Raleigh, NC



Small-Scale Commercial  
Raleigh, NC



Full-Scale Commercial  
Middlesex, NC





# Patented Platform Technologies

## Advanced food processing systems for liquid products

- ALL Electric energy
  - No Steam heating
- Allows for portability
- Can be right-sized for scalability
- Creates shelf-stable products
- Significant quality advantages – Nutrients, Color, Flavor
  - Examples: Babyfood, Smoothies, Fruit & Vegetable Puree, Nutrition Beverages

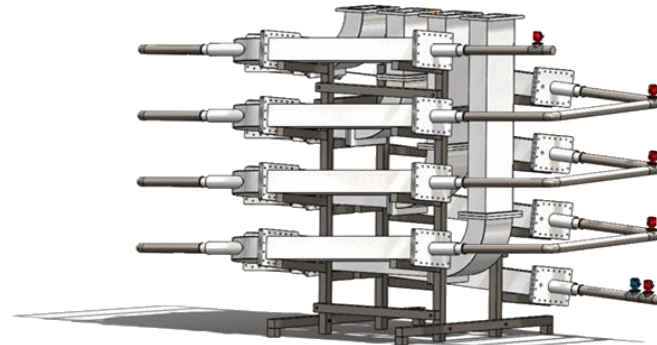
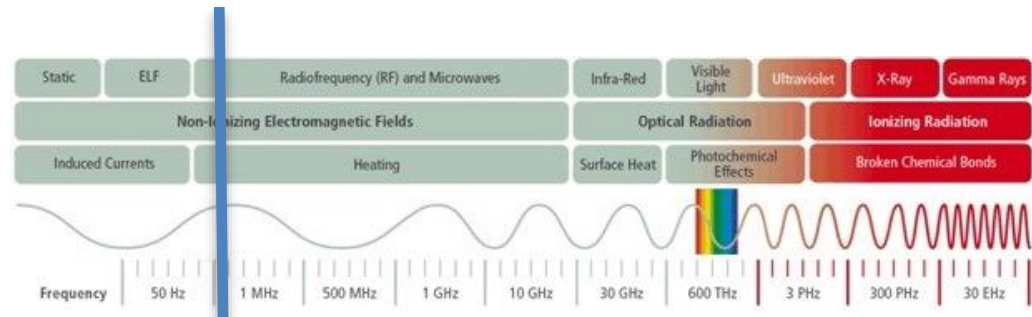




# Microwave Processing

## Microwave Heating:

- ✓ Safe
  - ✓ Fast
  - ✓ Gentle
  - ✓ Flexible
  - ✓ Efficient
  - ✓ Proven
- Enables pasteurization and sterilization of sensitive products





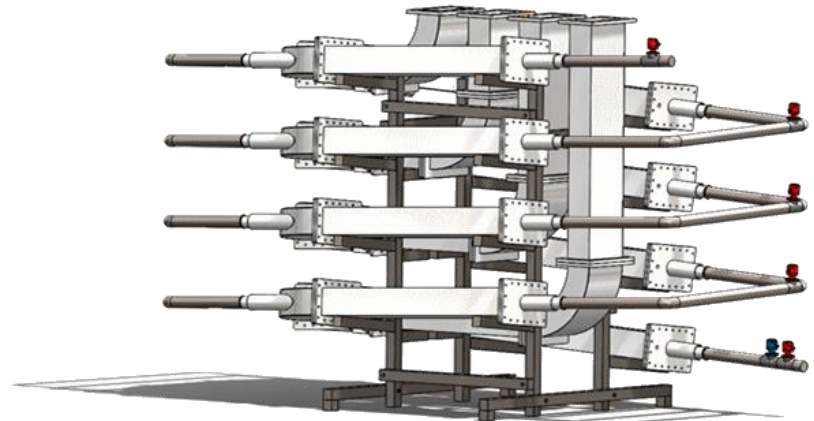
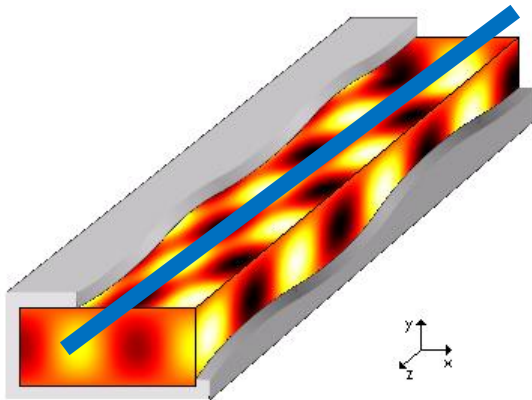


# Microwave Processing

## How it Works

Microwave Heating Principle:

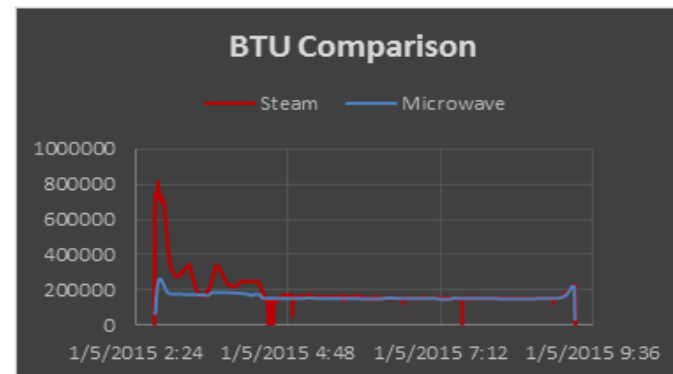
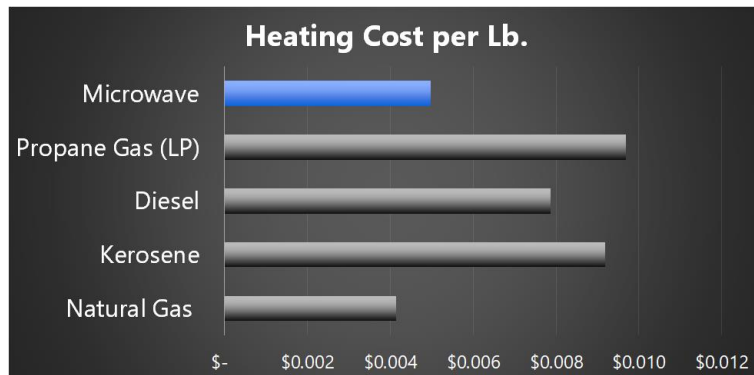
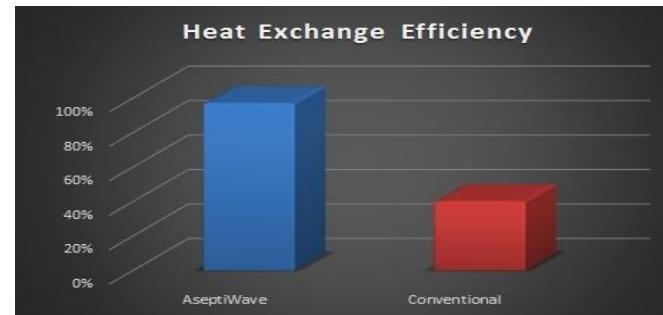
- ✓ Travelling Wave Applicators
- ✓ Even Consistent Heating with Electromagnetic Energy
- ✓ Able to Heat Any Viscosity or Particulate Size





# Microwave Processing - Energy Efficiency

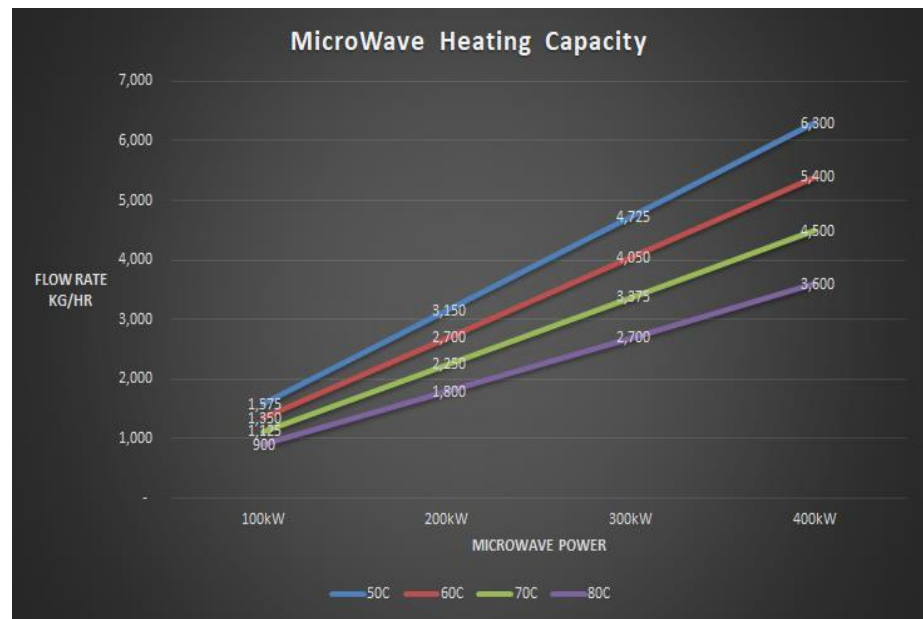
- ✓ Reduced energy consumption
- ✓ Reduced carbon footprint
- ✓ Faster Line startup
- ✓ Less downtime
- ✓ Low utility cost





## Microwave Processing - Energy Efficiency

- ✓ Precision Heating
- ✓ Scalable Design
- ✓ Can act as booster heater, final heater, or total heater
- ✓ Works well with regenerative pre-heating
- ✓ Greatest impact at higher temperatures where  $dT$  would be lowest in conventional heating.





# The Importance of a Strong Network

## Scaling Across the US:

- *Increasing Accessibility:* Our strategic expansion plan focuses on making aseptic processing accessible to smaller brands across the United States. This requires regionally located facilities instead of a large centralized facility.
- *Empowering Small Brands:* By eliminating MOQ, we empower smaller brands to bring their products to market with the precision and quality that was once reserved for large-scale manufacturers.
- Created the FirstWave Food Incubator to increase the odds of success for young brands



## The Importance of a Strong Network

- *Robust Data Security:* Commitment to a strong and secure network ensures that customers data is safeguarded. From critical thermal processing data, Lot traceability to regulatory information, we have to have a secure backbone.
- *Customer Information Protection:* So much of our clientele has priority information, and we have to ensure it is handled with the utmost care. Our network is fortified to protect sensitive customer data, building trust and loyalty.
- *Project Management Excellence:* With R&D handling over 50 projects concurrently and the commercialization team onboarding a dozen new clients at a time, our network ensures seamless collaboration, allowing for efficient project management.
- *Network Connectivity:* We need the ability to provide offsite support from our engineering team and provide live dashboards to share production data with customers and investors.



## Historicizing Critical Processing and Regulatory Information:

The FDA (Food and Drug Administration) has regulations regarding record-keeping for food manufacturing, which are outlined in the LACF (Low-Acid Canned Food) regulations. These guidelines are detailed in 21 CFR Part 113. Specifically, regarding document retention, the FDA requires that records related to the processing and production of low-acid canned foods be retained for a specific period of time.

- **Production and Process Records:** Records related to the production and processing of low-acid canned foods must be retained for a minimum of 3 years after the products were last distributed. These records should include information about the formulation, processing, packaging, and distribution of the products.
- **Distribution Records:** Records of the distribution of low-acid canned foods must also be kept for a minimum of 3 years. This includes information about where the products were distributed and to whom.
- **Complaint Files:** Any complaints regarding low-acid canned foods, including those related to illness or injury, must be documented and retained for a minimum of 3 years.
- **Records Accessibility:** These records should be readily available for inspection by FDA officials upon request.

## Recent cases of malware attacks on food manufacturing companies

- Mars Food: In June 2017, Mars, one of the world's largest food manufacturers, was reportedly affected by the Petya ransomware attack. The attack disrupted operations, and there were reports of some data being encrypted and held for ransom.
- Mondelez International: In June 2017, Mondelez, a major multinational food conglomerate, was also impacted by the Petya ransomware attack. The attack affected its global IT systems, including production facilities, causing disruptions.
- JBS USA: In May 2021, JBS USA, one of the world's largest meat processors, fell victim to a ransomware attack attributed to a Russian hacking group. The attack forced the temporary shutdown of several plants in the U.S., impacting meat production.
- Operational Disruption Costs: The most immediate and tangible cost is often related to the disruption of operations. This includes the downtime of manufacturing processes, logistics, and distribution, leading to potential revenue loss.
- Ransom Payments: In some cases, companies may choose to pay the ransom demanded by cybercriminals to regain access to their data and systems. The cost of ransom payments can vary widely.:
- Recovery and Remediation: Costs Restoring systems, conducting forensic investigations, and implementing cybersecurity improvements all contribute to the costs associated with recovering from a cyberattack.
- Legal and Regulatory Costs: Companies may face legal consequences and regulatory fines for failing to protect customer data or not adhering to cybersecurity regulations. Legal fees and compliance costs can be significant.
- Reputational Damage: The long-term impact on a company's reputation can result in loss of customers and business relationships. Rebuilding trust and reestablishing brand credibility often requires substantial investment in marketing and public relations efforts.



# Cybersecurity for Manufacturing Firms

Presented by:

**Eric Hobbs**

*President, Technology Associates*



# Topics

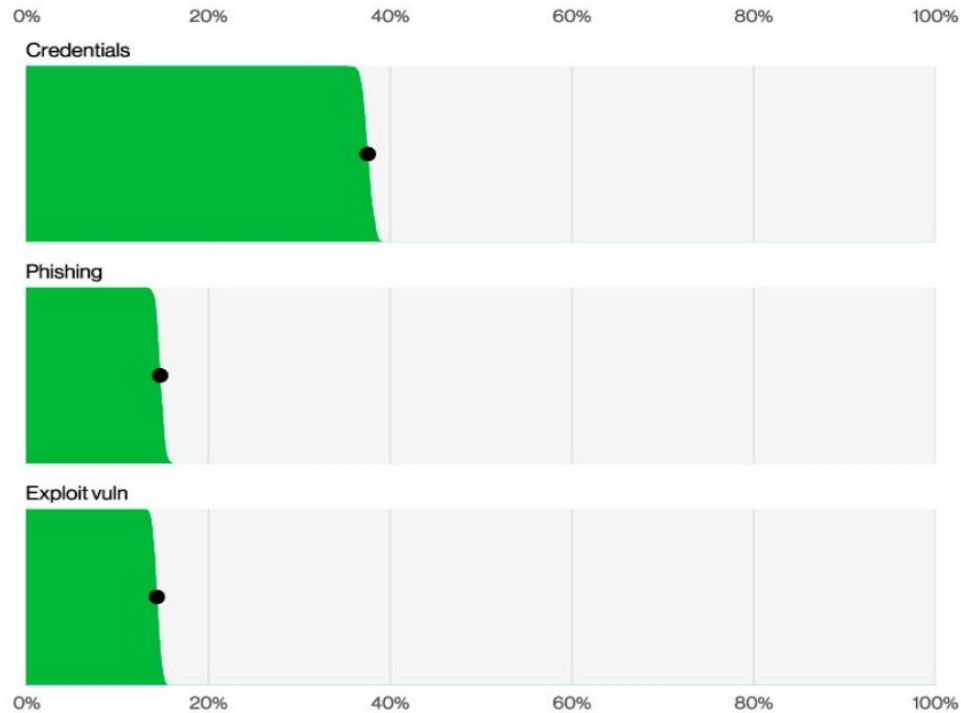
- Current cybersecurity threat landscape
- Financial impact
- Industry impact
- Risks you should focus on
- Security control framework
- Action steps to protect your company

# Current cybersecurity threat landscape

- Facts versus hype
- Real-world data
- Research
  - 2023 FBI Internet Crime Complain Center Report
  - 2023 Verizon Data Breach Investigations Report
- Terms
  - Incident - A security event that compromises the confidentiality, integrity or availability of an information asset
  - Breach - An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party

# Current cybersecurity threat landscape

- Overview (Entry Points)

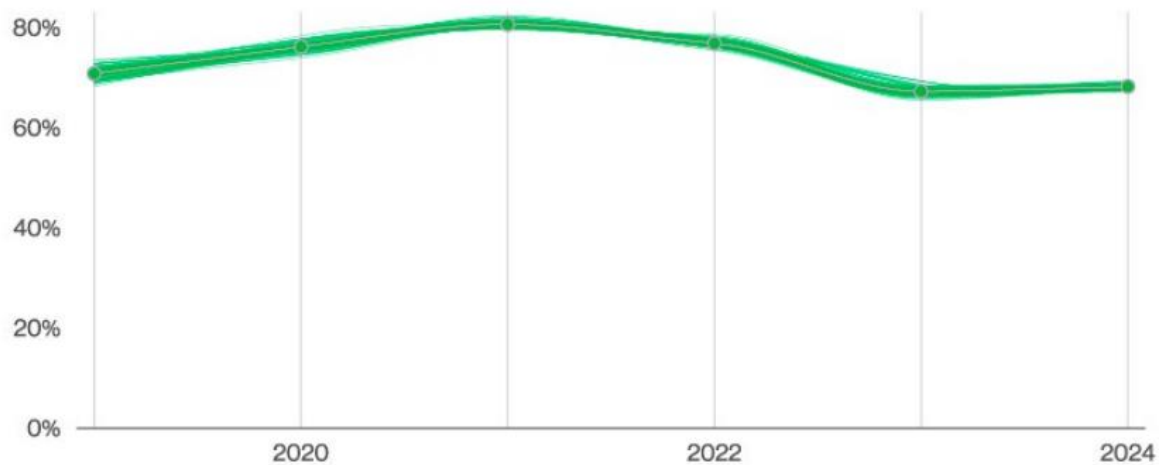


**Figure 1.** Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963)

Source: 2023 Verizon Data Breach Investigations Report

# Current cybersecurity threat landscape

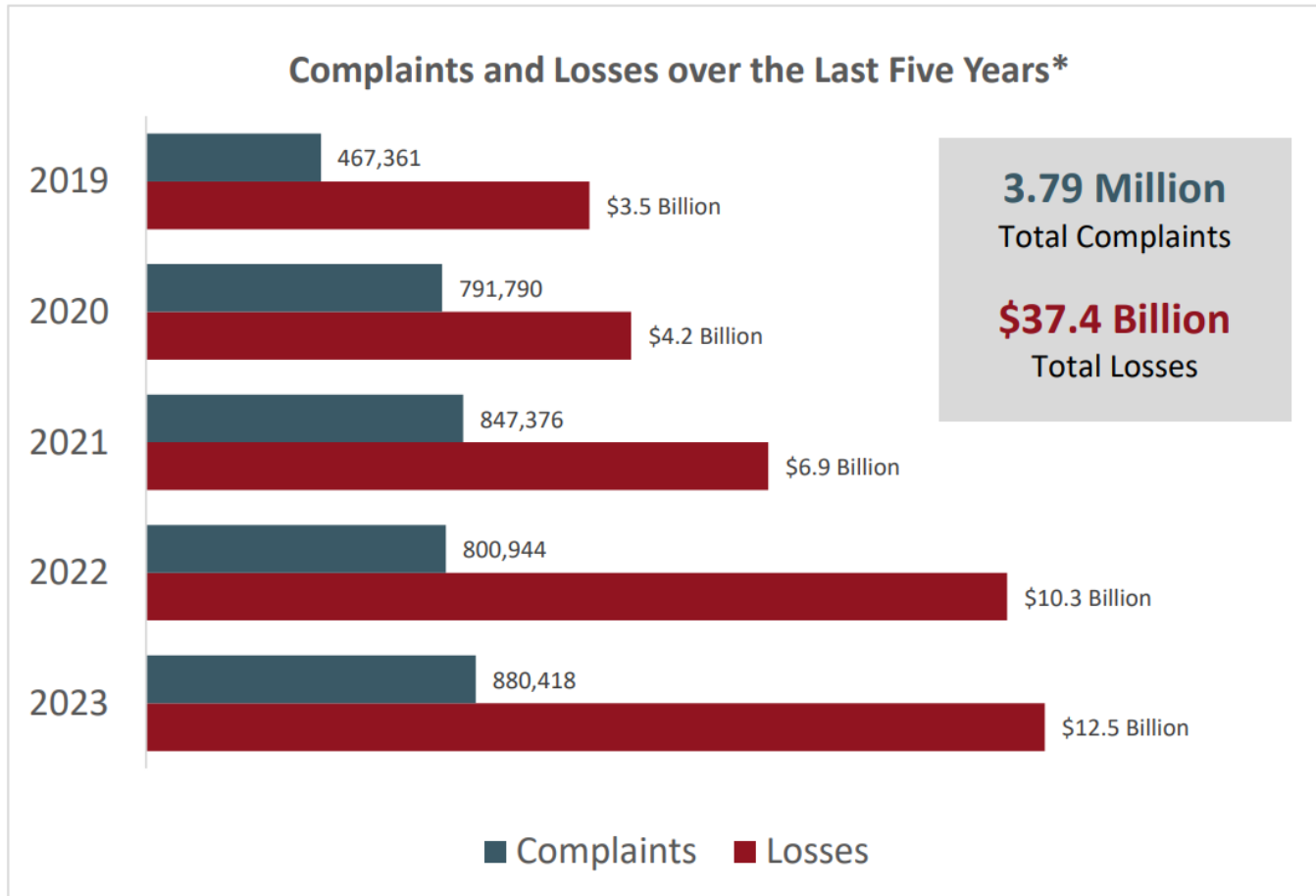
- Overview (The Human Element)



**Figure 8.** Human element enumeration in breaches over time

Source: 2023 Verizon Data Breach Investigations Report

# Financial Impact



Source: 2023 FBI IC3 Report

# Financial Impact

- FBI IC3 Report Highlights

## RANSOMWARE



In 2023, the IC3 received 2,825 complaints identified as ransomware with adjusted losses of more than \$59.6 million. Ransomware is a type of malicious software, or malware, that encrypts data on a computer, making it unusable. In addition to encrypting the network, the cyber-criminal will often steal data off the system and hold that data hostage until the ransom is paid. If the ransom is not paid, the entity's data remains unavailable.

## BUSINESS EMAIL COMPROMISE (BEC)



In 2023, the IC3 received 21,489 BEC complaints with adjusted losses over 2.9 billion. BEC is a sophisticated scam targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Source: 2023 FBI IC3 Report

# Industry Impact - 2023

Industry	Incidents				Breaches			
	Total	Small (1-1,000)	Large (1,000+)	Unknown	Total	Small (1-1,000)	Large (1,000+)	Unknown
Total	30,458	919	1,298	28,241	10,626	617	986	9,023
Accommodation (72)	220	16	9	195	106	16	9	81
Administrative (56)	28	7	7	14	21	6	4	11
Agriculture (11)	79	5	0	74	56	4	0	52
Construction (23)	249	17	6	226	220	12	5	203
Education (61)	1,780	82	630	1,068	1,537	56	618	863
Entertainment (71)	447	16	2	429	306	10	1	295
Finance (52)	3,348	75	122	3,151	1,115	54	87	974
Healthcare (62)	1,378	54	21	1,303	1,220	41	18	1,161
Information (51)	1,367	79	62	1,226	602	49	19	534
Management (55)	22	4	1	17	19	4	1	14
Manufacturing (31-33)	2,305	102	81	2,122	849	62	49	738
Mining (21)	30	1	2	27	20	1	1	18
Other Services (81)	462	13	5	444	417	8	5	404
Professional (54)	2,599	205	102	2,292	1,314	124	73	1,117
Public Administration (92)	12,217	56	115	12,046	1,085	39	27	1,019
Real Estate (53)	432	35	5	392	399	29	2	368
Retail (44-45)	725	90	47	588	369	55	32	282
Transportation (48-49)	260	21	38	201	138	17	12	109
Utilities (22)	191	17	11	163	130	12	6	112
Wholesale Trade (42)	76	22	21	33	54	17	14	23
Unknown	2,243	2	11	2,230	649	1	3	645
Total	30,458	919	1,298	28,241	10,626	617	986	9,023

**Table 2.** Number of security incidents and breaches by victim industry and organization size

Source: 2023 Verizon Data Breach Investigations Report

# Risks you should focus on

- An employee or vendor changes routing information of a transfer
- An employee gives up their credentials via a phishing attempt
- An employee opens an email attachment allowing C2 / Ransomware to be installed
- Bad Password policies and lack of multifactor lead to cross-platform password breach



# Risks you should focus on

- **Understand that humans are a key element in security.** Humans are often considered the weakest element in any security solution. No matter what physical or logical controls are deployed, humans can discover ways to avoid them, circumvent or subvert them, or disable them. However, people can also become a key security asset when they are properly trained and are motivated to protect not only themselves but the security of the organization as well." - *Certified Information Systems Security Professional Official Study Guide, 9th Edition*

# Risks you should focus on

- “We use MFA so we are good...”



Dear [Name],

We are sending a friendly second reminder to let you know that your password for Office 365, provided by Voltone SP, is set to expire in 72 hours.

**Your IT administrator has recently enacted a policy within our systems that require all users to reset their Office 365 password every 90 days, in accordance with the policies within the Voltone SP .**

Please click

[here](#)

to log into Office 365 to change your password.

Sincerely,

*The Azure Active Directory Team*

Microsoft Inc | Two Microsoft Road Seattle, WA 98562-6300

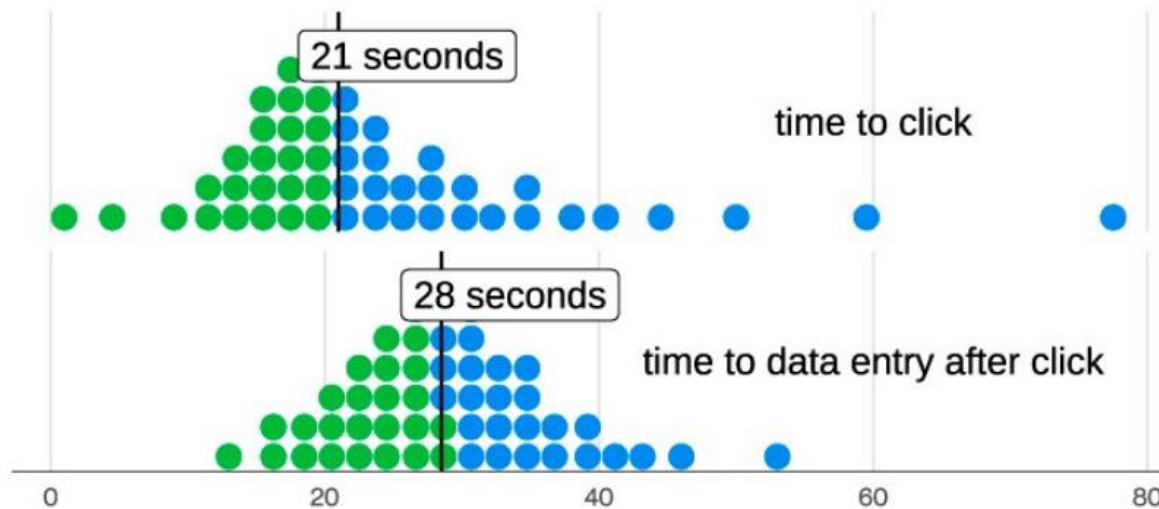
This message was sent from an unmonitored email address. Please do not reply to this message.

**Microsoft**

[Privacy](#) | [Legal](#)

# Risks you should focus on

- “We use MFA so we are good...”



**Figure 39.** Time between email clicked and data entered

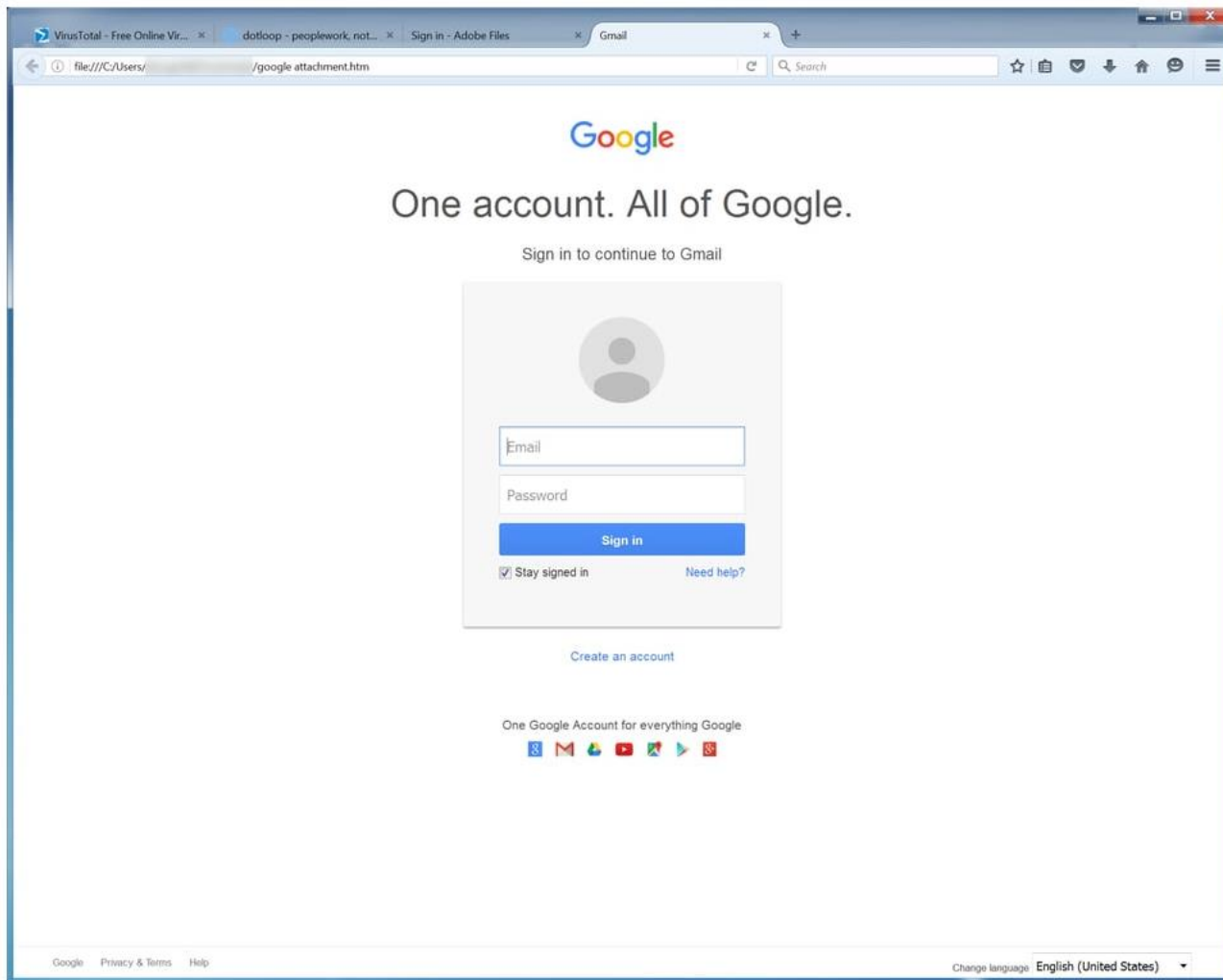
2023 Verizon Data Breach Investigations Report

# Risks you should focus on

Q2 Forecast and Financials:- 0047

Fw: V

deliver:  
to me



The screenshot shows a web browser window with the Gmail sign-in page. The browser's address bar contains the URL `file:///C:/Users/.../google attachment.htm`. The page features the Google logo at the top, followed by the text "One account. All of Google." and "Sign in to continue to Gmail". Below this is a sign-in form with fields for "Email" and "Password", a blue "Sign in" button, and a checkbox for "Stay signed in" with a "Need help?" link. At the bottom of the form is a "Create an account" link. Below the form, it says "One Google Account for everything Google" with icons for various Google services. The footer of the page includes "Google Privacy & Terms Help" and a language selector set to "English (United States)".

Microsoft

# Security Control Framework

- SOC 2
- HIPAA
- HITRUST
- COBIT
- NERC-CIP
- FISMA
- CCPA
- CIS Controls
- **ISO 27001(27701)**
- **NIST 800-53**
- **NIST 800-171**
- **NIST CSF \***
- **PCI DSS**
- **GDPR**

# Security Control Frameworks

- NIST Cybersecurity Framework (CSF)
  - "Go-to" controls framework for private industry
  - Aligns with NIST 800-53/171
  - More flexible / understandable
  - [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)
  - NISTIR 8183r1
    - Cybersecurity Framework Manufacturing Profile

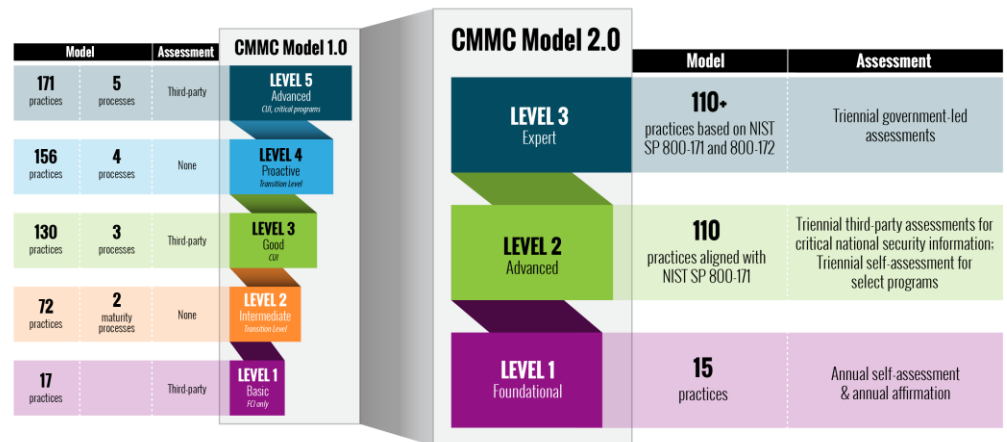
# Security Control Frameworks

- NIST Cybersecurity Framework (CSF) 2.0
- Govern – “The organization’s cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored”



# Security Control Frameworks

- CMMC 2.0
  - Largely based on NIST 800-53 / 800-171
  - Allows Plan of Action / Milestones (180 days)
  - DD Form 254 – CUI checkbox
  - When?
    - ~~Finalized May 2023~~
    - ~~Contracts July 2023~~
    - Contracts Oct. 2024





# Security Control Frameworks

- CMMC 2.0 - Enclave
  - According to DoD: “When implementing CMMC, a DIB contractor can achieve a specific CMMC level for its entire enterprise network or for a particular segment(s) or enclave(s) depending upon where the information to be protected is handled and stored.”
  - According to NIST: “Isolating CUI into its own security domain by applying architectural design concepts may be the most cost-effective and efficient approach for non-federal organizations to satisfy the security requirements and protect the confidentiality of CUI.”

# Action steps to protect your company

- **Don't** Trust but Verify
  - FBI IC3: "Procedures should be put in place to verify payments and purchase requests outside of e-mail communication and can include direct phone calls but to a known verified number and not relying on information or phone numbers included in the e-mail communication."
  - FBI IC3: "Never make any payment changes without verifying the change with the intended recipient..."

# Action steps to protect your company

- Operational
  - Ongoing User Training, Education and Testing
  - Verification procedures - PUTP
- Technical
  - Multi-Factor Authentication
  - REAL anti-phishing / threat intelligence system
- Management
  - Top-Down
  - Security Framework

# Action steps to protect your company

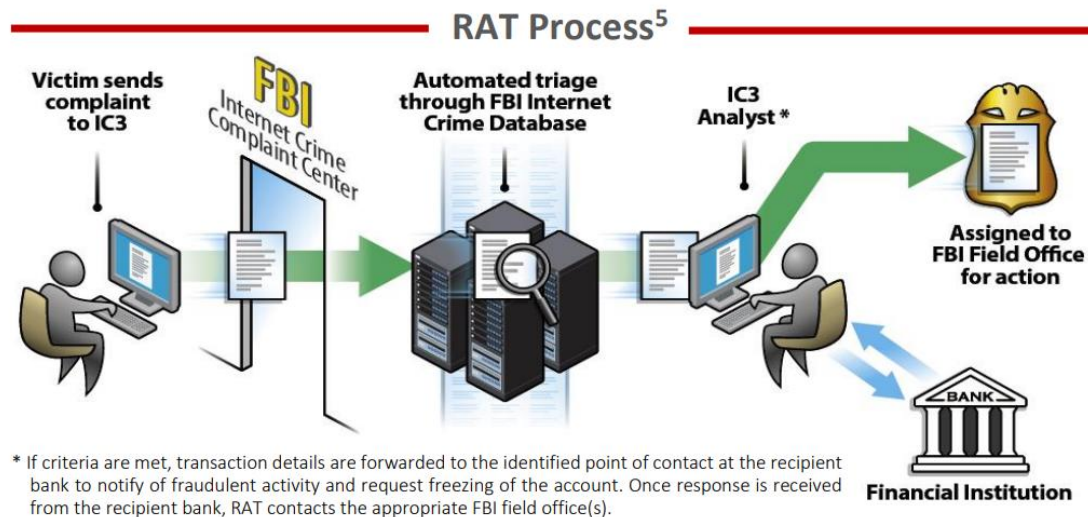
- Security Framework
  - International customers and/or already on ISO 9001 path? Go with ISO - 27701
  - If not? NIST CSF
  
- CMMC
  - Only if I had to, ex: DoD CUI confirmed
  - Then enclave

# Special Note

- RAT – ic3.gov

## THE IC3 RECOVERY ASSET TEAM (RAT)

The Internet Crime Complaint Center's Recovery Asset Team (RAT) was established in February 2018 to streamline communication with financial institutions and assist FBI field offices with the freezing of funds for those who made transfers to domestic accounts under fraudulent pretenses.



The RAT functions as a liaison between law enforcement and financial institutions supporting statistical and investigative analysis.

# Thank you!

Further Questions?

Eric Hobbs

[ehobbs@technologyassociates.net](mailto:ehobbs@technologyassociates.net)

<https://www.linkedin.com/in/hobbseric/>