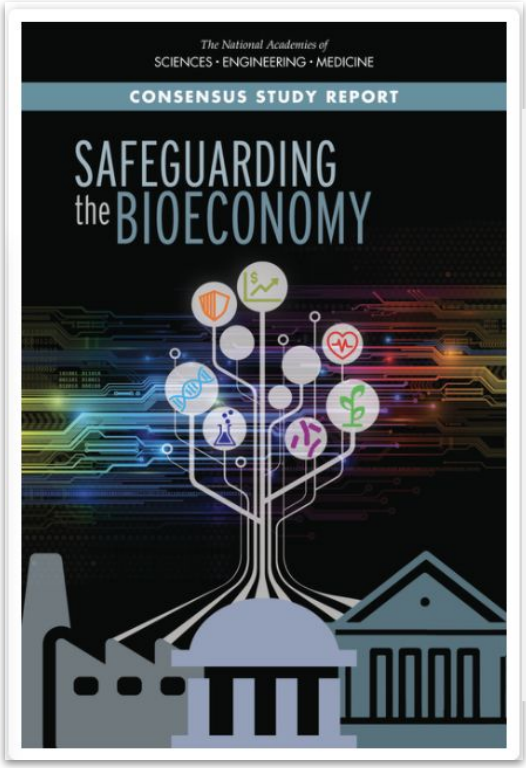
bioisac
Creating Collaborative Threat Intelligence for the Bioeconomy

Understanding Cyberbiosecurity

Whitney Zatzkin - September 2026
whitney@isac.bio

Disclosures: tips@isac.bio
PGP: EB2AA1AA4AD94A0BBE07 E8A9625BBFEE2E95C7FC
Need emergency help? Email help@isac.bio to receive timely help

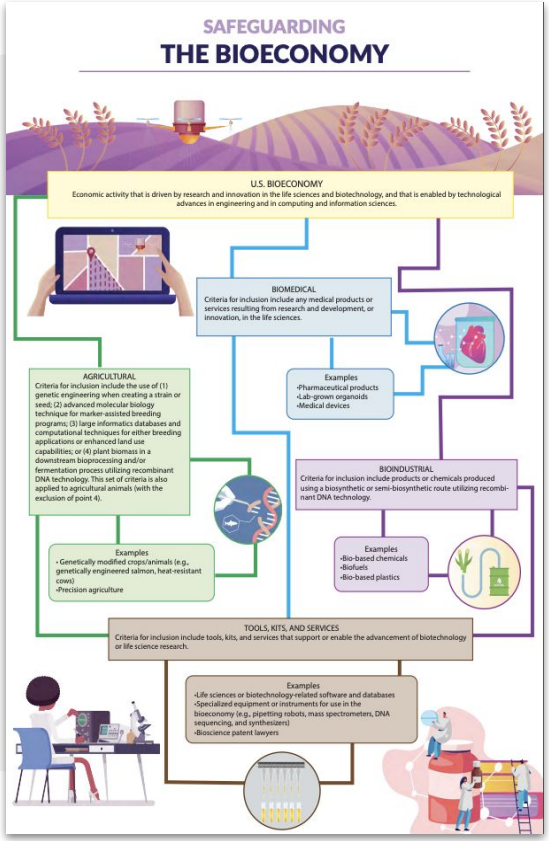
Answering the Call



https://bit.ly/NAMBioeconomy

January 2020

Recommendation 8: Bioeconomy stakeholders should pursue membership in one or more relevant information sharing and analysis centers (ISACs)...or **consider creating a new sector-based information-sharing organization for members of the bioeconomy.** [CISA] within the U.S. Department of Homeland Security should convene bioeconomy stakeholders to build awareness about relevant models for sharing information on cyber threats. Those convened should consider whether an active repository is needed to host and maintain key bioeconomy-related open source software, algorithm components, and datasets.



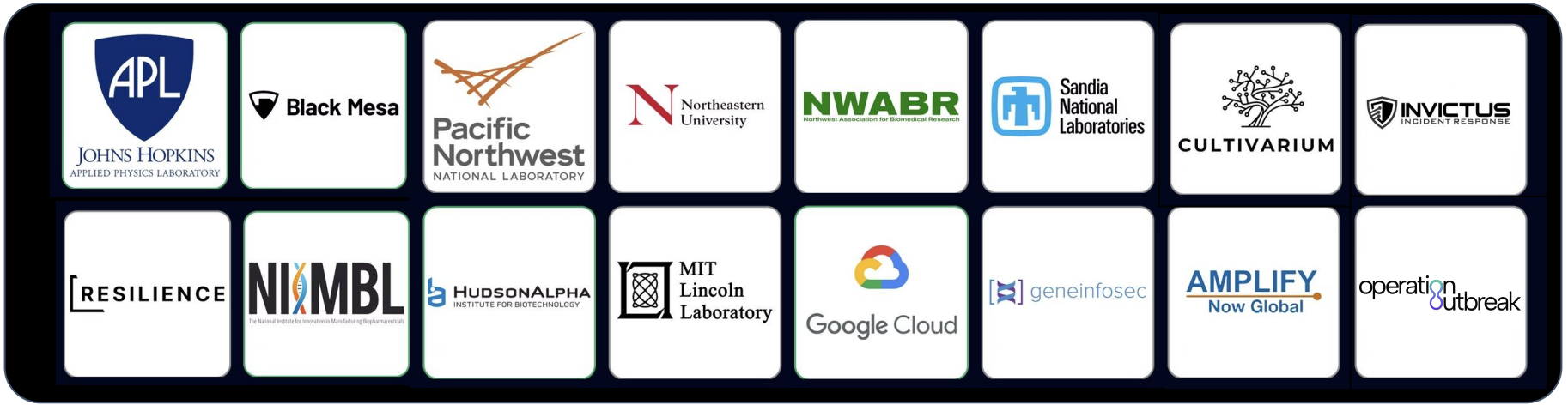
DO NOT DISTRIBUTE

BIO-ISAC

The **Bioeconomy Information Sharing and Analysis Center addresses threats unique to the bioeconomy** and enables coordination among stakeholders to facilitate a resilient and secure industry. BIO-ISAC provides two-way sharing of intelligence among public and private organizations, including AI, biotechnology and biomanufacturing, **serving as the global resource for information on cyberbiosecurity threats**. (isac.bio)

help@isac.bio

Experiential trainings for Public/Private sector	Confidential incident support, responsible disclosure	Publish secure guides, best practices, and resources	High-trust, not for attribution, regional groups



DO NOT DISTRIBUTE

Everyone.
Take a deep breath.

DO NOT DISTRIBUTE

What does a cyberbiosecurity incident feel like?

DO NOT DISTRIBUTE

What does a cyberbiosecurity incident feel like?

Let's find out!

DO NOT DISTRIBUTE

Cyberbiosecurity Incident

YOU are a member of the biopharma manufacturing team for a very successful diabetes drug (GLP-1). *(yay!)*

Routine security scans of the manufacturing equipment show the **need to investigate** a specific instrument. It generates $1M/week. *(hrmm.)*

DO NOT DISTRIBUTE

Cyberbiosecurity Incident

YOU are a member of the biopharma manufacturing team for a very successful diabetes drug (GLP-1). *(yay!)*

Routine security scans of the manufacturing equipment show the **need to investigate** a specific instrument. It generates $1M/week. *(hrmm.)*

To investigate, this instrument would be pulled for an **undetermined amount of time** and will **impact global manufacturing timelines**, and stockpiles, and patient care. It will require **regulatory reports** and auditing, and possibly require you to **notify contract holders**. *(yikes.)*

DO NOT DISTRIBUTE

Cyberbiosecurity Incident

YOU are a member of the biopharma manufacturing team for a very successful diabetes drug (GLP-1). *(yay!)*

Routine security scans of the manufacturing equipment show the **need to investigate** a specific instrument. It generates $1M/week. *(hrmm.)*

To investigate, this instrument would be pulled for an **undetermined amount of time** and will **impact global manufacturing timelines**, and stockpiles, and patient care. It will require **regulatory reports** and auditing, and possibly require you to **notify contract holders**. *(yikes.)*

You learn your scientists **brought in personal hotspots** because the security team didn't let them access gmail during the workday. You decide to examine the equipment. **You find there's a threat actor.** *(uh oh!)*
You learn a **security patch** conducted by a third-party caused it.
You want to **protect people** and **make money** – what do you do? *(ugh!)*

DO NOT DISTRIBUTE

Cyberbiosecurity Incident

YOU are a member of the biopharma manufacturing team for a very successful diabetes drug (GLP-1). *(yay!)*

Routine security scans of the manufacturing equipment show the **need to investigate** a specific instrument. It generates $1M/week. *(hrmm.)*

To investigate, this instrument would be pulled for an **undetermined amount of time** and will **impact global manufacturing timelines**, and stockpiles, and patient care. It will require **regulatory reports** and auditing, and possibly require you to **notify contract holders**. *(yikes.)*

You learn your scientists **brought in personal hotspots** because the security team didn't let them access gmail during the workday. You decide to examine the equipment. **You find there's a threat actor.** *(uh oh!)*
You learn a **security patch** conducted by a third-party caused it.
You want to **protect patients** and **make money.** *(ugh!)*

Do you **fix it**? **Ignore it** and keep manufacturing? **Share IP** with a competitor?
Buy parts on eBay? Tell no one? **Run away**?

DO NOT DISTRIBUTE

Holy Smokes!

DO NOT DISTRIBUTE

That couldn’t *actually* happen.

DO NOT DISTRIBUTE

That couldn't *actually* happen.

Are you sure?

DO NOT DISTRIBUTE

Meet Tardigrade

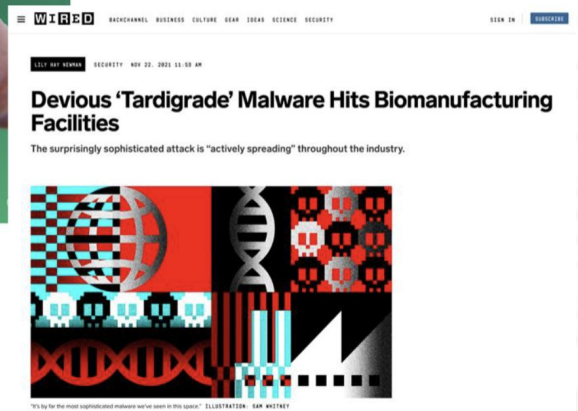
It did.

Spring 2021 - Ongoing

Thankfully, they acted within hours and called BIO-ISAC (help@isac.bio).

We had a team investigating in an hour and on the ground within 3 days, navigating a border crossing via personal relationships.





1. A routine scan showed something
2. Further evaluation revealed a cyber attack
3. **Significant impacts to vaccine production**, revenues, and the industry/economy
4. Federal regulations and responses **did not match expectations**
5. This threat persists, globally, today

Source: isac.bio/post/tardigrade

DO NOT DISTRIBUTE

Okay, fine.
But it's just *one* case.

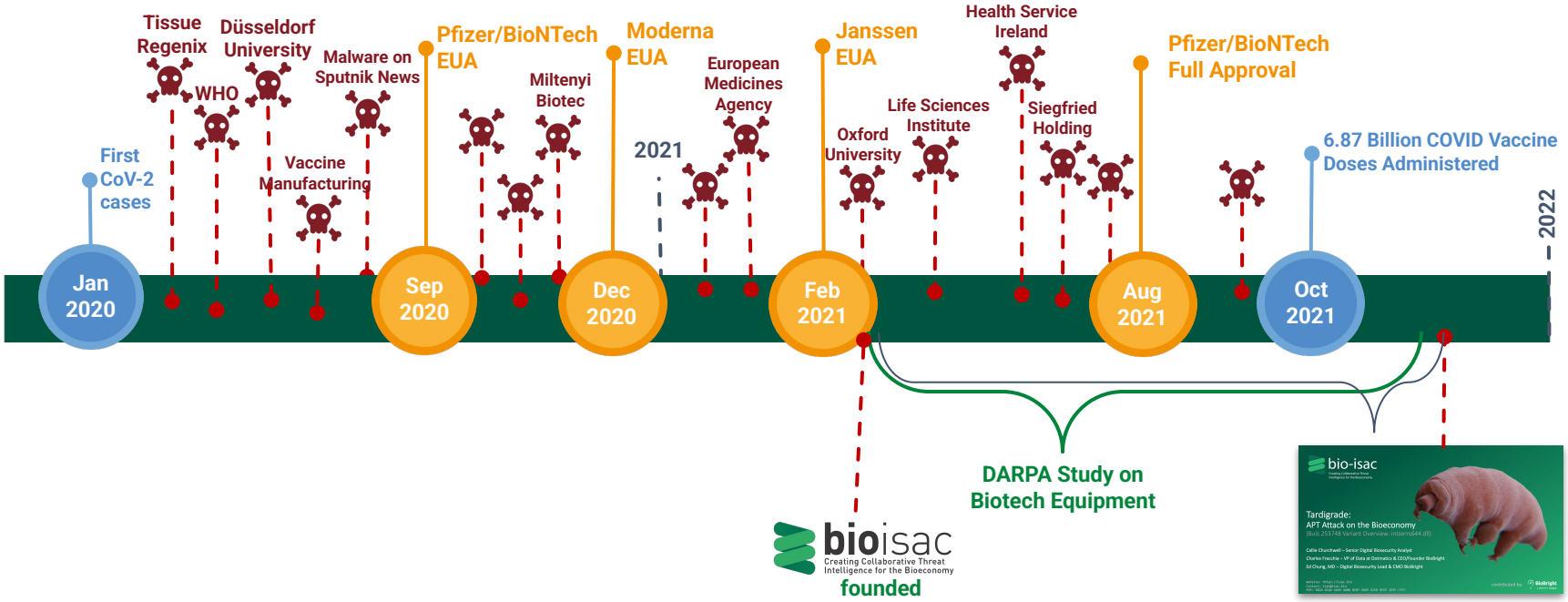
DO NOT DISTRIBUTE

Okay, fine.
But it's just *one* case.

Are you sure?

DO NOT DISTRIBUTE

Retrospective Analysis: Attacks during SARS CoV-2



Got it.

So *biopharma* needs to do a better job.

DO NOT DISTRIBUTE

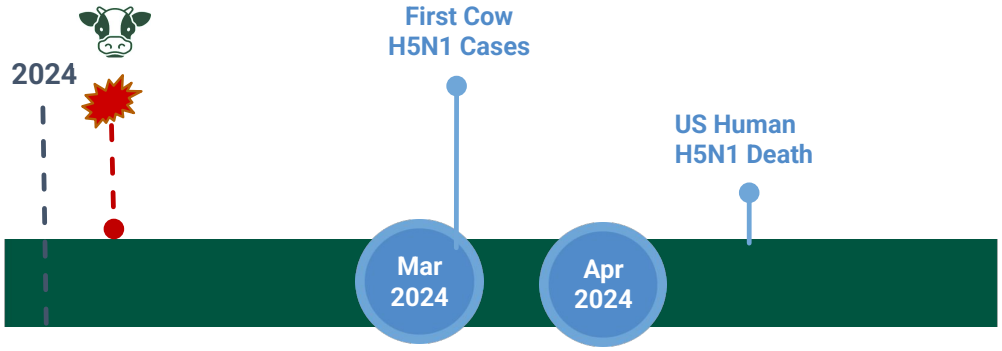
Got it.

So *biopharma* needs to do a better job.

Are you sure?

DO NOT DISTRIBUTE

Connecting to Cows





In January 2024, some folks contacted BIO-ISAC about (self-determined) HPAI in their cows (and staff!). *(We reported this immediately to US regulators!)*

We grew curious about the cyber components of the industry.
Using the same methodology, we made a list of known cyber attacks in dairy, tracked the threat actors then/now, and then explored for signs of industry-wide risk.

Retrospective Analysis: Attacks during SARS CoV-2

bioisac
Creating Collaborative Threat Intelligence for the Bioeconomy

2020
First CoV-2 cases
Jan 2020
Tissue Regenix
WHO
Düsseldorf University
Vaccine Manufacturing
Malware on Sputnik News
Pfizer/BioNTech EUA
Sep 2020
Miltenyi Biotec
Moderna EUA
Dec 2020
2021
European Medicines Agency
Janssen EUA
Feb 2021
Oxford University
Life Sciences Institute
Health Service Ireland
Siegfried Holding
Pfizer/BioNTech Full Approval
Aug 2021
6.87 Billion Doses Administered
Oct 2021
2022

Lanco-Pennland
(unknown, first disclosed BIO-ISAC Feb 2024)

Americold 1

Dairy Farm Group
(REvil)

Lactalis
(unknown)

JBS (meat)
(REvil)

DARPA Study on BioTech Equipment

Schreiber
(BlackMatter)

Analysis: Attacks in Agri during HPAI/Cattle

2022
Rice Fruit
BIO-ISAC disclosure

Hood Dairy
(unknown)

2023
Americold 2
(Cactus)

2024
(REvil)

Kasseika
(BlackMatter Resurfaces)

First Cow H5N1 Cases
Mar 2024

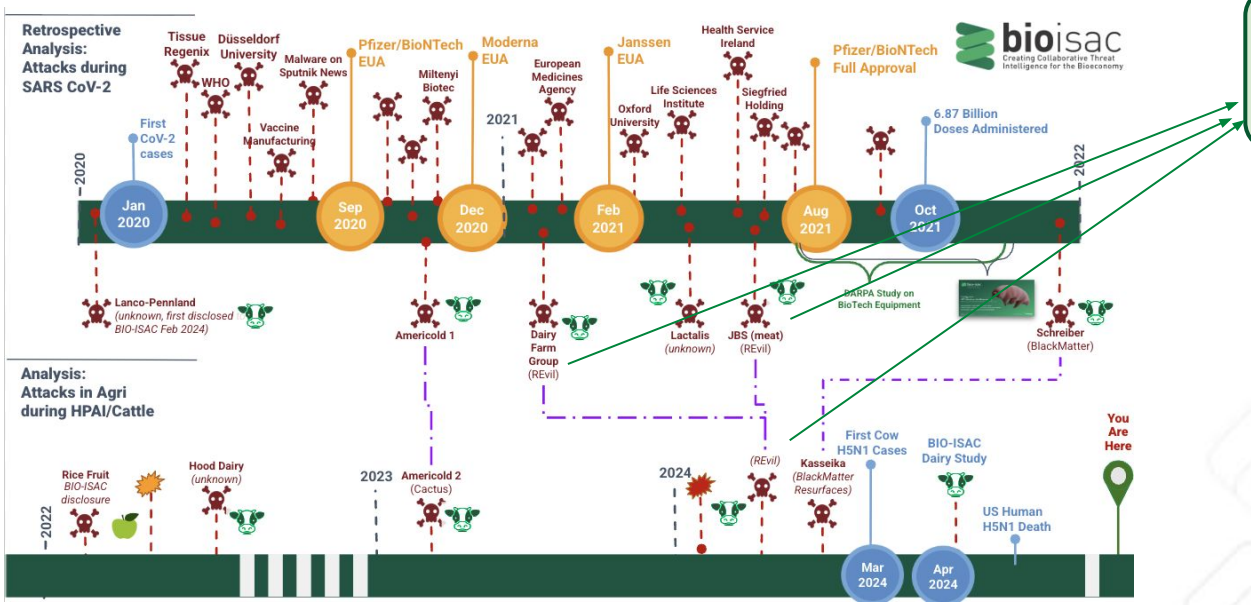
BIO-ISAC Dairy Study
Apr 2024

US Human H5N1 Death

You Are Here

DO NOT DISTRIBUTE

The attackers from 2021, resurfaced.



REvil attacked Dairy Farm Group and JBS. After some were released from jail, they tested new attacks at an ATM machine in London.

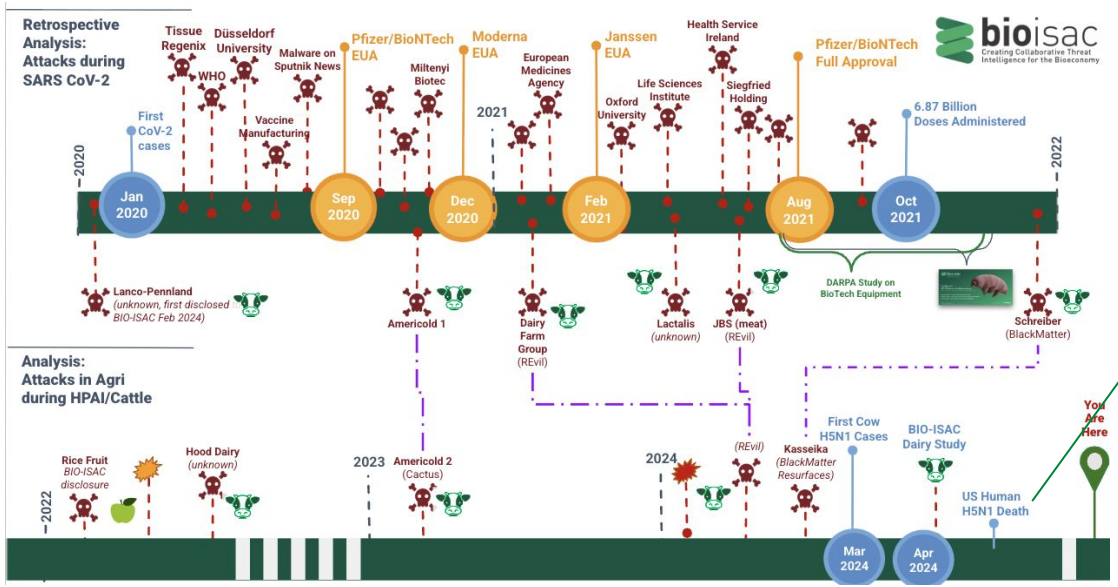
At sentencing, they were making **$100M a year.**

List of ransomware group PR pages:

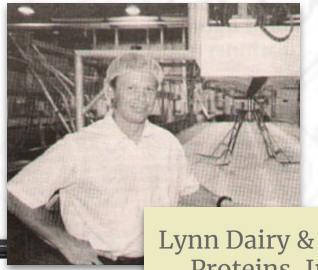


Though many threat actors went to jail, they **returned to attacking once released**. We know this because **they issued press releases.**

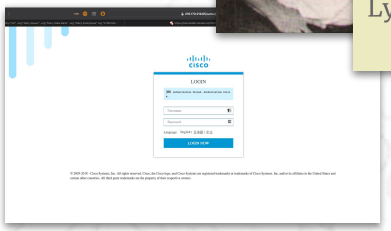
Exposure Online



From checking a free (legal!) online web scanning tool, we saw:
216.170.219.65
Lynn Dairy Inc. USA



Lynn Dairy & Lynn Proteins, Inc.



We had **concerns about the connected equipment caring for the animals and the technology used in dairy processing** (SCADA, thermometers, refrigeration, etc).

We **confirmed active vulnerabilities at at least 40 US dairy sites** (open IPs, patches due). **15% of those had attacks a year later.**

Ethical researchers stop here.
Do the bad guys?
Does AI?

What does this mean in the real world?

The following attacks are not fictional scenarios.

This is about the abuse of things meant to protect.

DO NOT DISTRIBUTE

Real world evidence: ransomware

Ransomware is software used to disable your computer, unless you pay money to the attacker.

GROCERY DIVE Deep Dive Opinion Library Events Press Releases Topics

UNFI services disrupted by cyberattack

The grocery retailer and wholesaler is working to resume full operations following "unauthorized activity" involving its IT systems.

Published June 9, 2025

REUTERS World Business Markets Sustainability More

Business

AGCO ransomware attack disrupts tractor sales during U.S. planting season

By Bianca Flowers and Nathan Gomes

May 6, 2022 4:34 PM EDT · Updated 2 years ago

Law Firm Investigates AGCO Following Ransomware Attack

May 24, 2022 | Posted in Manufacturer News

Source: Accesswire

NEW YORK, NY, May 23, 2022 — Pomerantz Law Firm is investigating claims on behalf of investors of AGCO Corporation. The investigation concerns whether AGCO and certain officers and/or directors have engaged in securities fraud or other unlawful business practices.

On May 6, 2022, AGCO disclosed that it expects operations at some of its production facilities to be affected for "several days and potentially longer" following a ransomware attack. On this news, AGCO's stock price fell $7.53 per share, or 5.76%, to close at $123.30 per share May 6, 2022.

ars TECHNICA

Iowa-based provider of agriculture services NEW Cooperative Inc. has been hit by a ransomware attack, forcing it to take its systems offline. The BlackMatter group that is behind the attack has put forth a $5.9 million ransom demand. The farming cooperative is seen stating the attack could significantly impact the public supply of grain, pork, and chicken if it cannot bring its systems back online.

BlackMatter says it doesn't hit "critical infrastructure"

Ransomware group BlackMatter has hit NEW Cooperative and is demanding $5.9 million to provide a decryptor, according to screenshots shared online by threat intel analysts.

"Your website says you do not attack critical infrastructure. We are critical infrastructure... intertwined with the food supply chain in the US. If we are not able to recover very shortly, there is going to be very very public disruption to the grain, pork, and chicken supply chain," a NEW Cooperative representative appears to be telling BlackMatter during a private negotiation chat.

The farming organization says its software powers about 40 percent of grain production and feed schedules of 11 million farm animals. And, as such, US federal government regulators like CISA may soon step in should the cooperative's systems not come back online soon.

$5.9 million @ NEW Cooperative

Crystal Valley Cooperative becomes latest agriculture business hit with ransomware

The company released a statement on Tuesday evening, but its websites are now down.



Written by **Jonathan Greig,** Contributor

Sept. 22, 2021 at 9:42 a.m. PT

$5.9 million @ Crystal Valley

DO NOT DISTRIBUTE

Real world evidence: livestock and food as ransom

Attacks impact operations and full crop seasons, livestock.

CALGARY HERALD

National / Business

Safety Net: A flock of chickens, held for ransom — Growing cyberattacks on Canada's food system threaten disaster

The domestic food production system may actually be one of the most glaring cracks in Canada's national defences

In other cases, it's more sophisticated. Twice, Dehghantanha has seen hackers break into a farm system and threaten to kill livestock — chickens in one case, cattle in another. And in about a third of the investigations his team as conducted over the past year, he has found evidence that state-sponsored hackers from Russia, China, North Korea and Iran have figured out how to quietly gain access to a control system inside a farm.

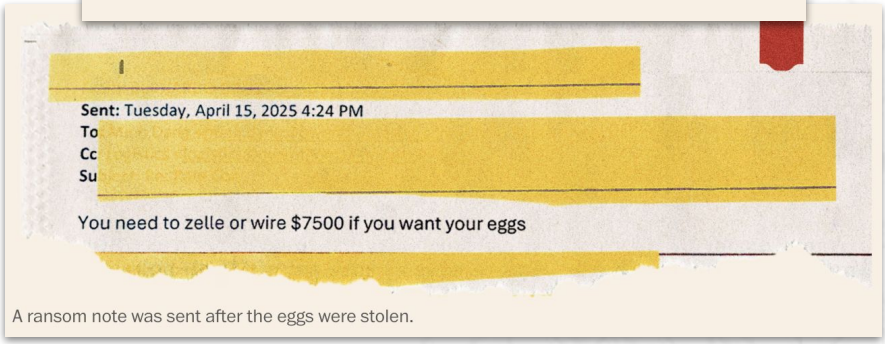
THE GREAT EGG HEIST

280,000 eggs disappeared from America's top producer. Then came a ransom note.

By Jenn Abelson and Jessica Contrera

Illustrations by Maria Alconada Brooks

June 19, 2025



A ransom note was sent after the eggs were stolen.

Real world evidence: cyber attacks means food shortages

Attacks impact production volume and delivery.

CNN BUSINESS Audio Live TV

(CNN) — A cyberattack earlier this month forced produce giant Dole to temporarily shut down production plants in North America and halt food shipments to grocery stores, according to a company memo about the incident obtained by CNN.

A cyberattack on Dole was the cause of the salad shortage, Adam Wolfe, the store's manager, told CNN, citing the Dole memo, which he said his store received from its wholesale grocery provider, Affiliated Foods Inc., in Texas.

down our systems throughout North America," Emanuel Lazopoulos, senior vice president at Dole's Fresh Vegetables division, said in a February 10 memo to retailers.

Media Statement: JBS USA Cybersecurity Attack

May 31, 2021 16:07 ET| Source: JBS USA, LLC Follow

GREELEY, Colo., May 31, 2021 (GLOBE NEWSWIRE) -- On Sunday, May 30, JBS USA determined that it was the target of an organized

Beef Central also reported that the price for a U.S. boxed beef cutout went up by $3/cwt (a standard unit of weight) for Choice, and 5.55 cents for Select grade on June 1 compared with May 28.

were not affected, and it is actively working with an Incident Response firm to restore its systems as soon as possible.

TRENDING NOW

Food shortages, Dutch supermarkets missing stock after ransomware attack

April 15, 2021

Items missing from shelves included packaged cheese. Grated cheese, sliced cheese, cream brie...etc. "Cheese deliveries were reportedly held up for three days, creating a backlog of orders and supermarket shortages".

Hackers hit Hood. Dairy shut down milk production this week after 'cyber security event.'

Dairy says plants are 'getting back up and running' but N.H. school district warns milk supply could be delayed

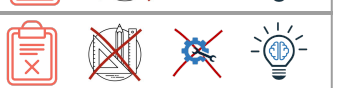
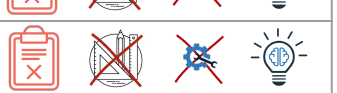
By Anissa Gardizy Globe Staff, Updated March 18, 2022, 12:39 p.m. 19

We are vulnerable everywhere we connect.

DO NOT DISTRIBUTE

Real world evidence: Verified Vulnerable Equipment (DARPA funded)

Barcode Readers	
Thermometers	
Flow Cytometer	
Laboratory/Production Automation	
Bioreactors	
Liquid Chromatography	
Pumps (in biomanufacturing)	 ~~~2023~~~
Liquid Handler	 ~2026
USBs (ports, drives) **DO NOT USE!**	

Electronic Batch Record Systems	
SCADA/Historians	
Sequencers	
Synthesizers	

- **Virtually all QA/QC methods are vulnerable to simple and devastating digital attacks.**
- **GxP compliance requires that equipment stays vulnerable.**
- **“Air gapping” lab equipment is false security.** *(How does software get updated? Data sharing?)*

 data/product can be manipulated remotely

 vendor contacted, not fixing

 vendor promises fix in 18+ mos.

 design/manufacturing vulnerability

 known to be exploited

 software exploited elsewhere

 further study needed

This is about eroding trust.

DO NOT DISTRIBUTE

Real world evidence: Incidents repeat themselves

Attacks repeat themselves, making the site, itself, a vulnerability.

June 2022

April 2023

May 2024

November 2020

May 2023

Aug 2022

Jan 2025

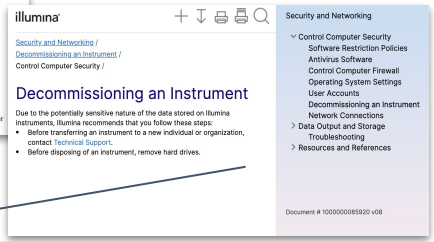
Jan 2025

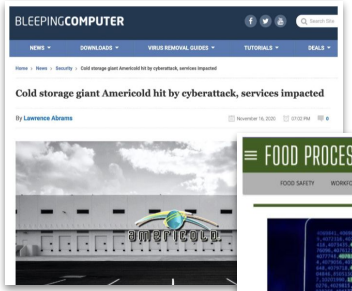
For reasons, a media sanitization alert

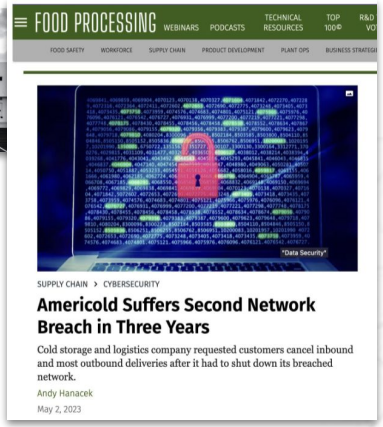


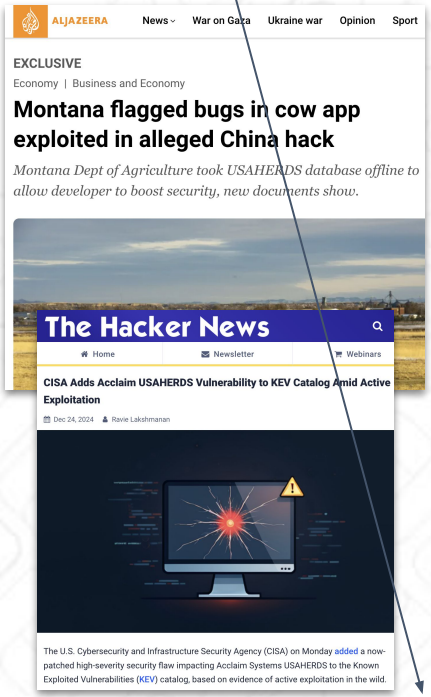












DO NOT DISTRIBUTE

Real world evidence: Impersonating public figures



Canadian Anti-Fraud Centre

Canada

Search

Browse frauds | Protect yourself | Report fraud | What to do if you're a victim

Home

Joint Advisory: Cyber officials warn Canadians of malicious campaign to impersonate high-profile public figures

June 23, 2025
Canadian Centre for Cyber Security (CCCS)
Canadian Anti-Fraud Centre (CAFC)

Cyber security officials in the Government of Canada are warning Canadians about a spike in malicious cyber activity, where threat actors are using text and AI-generated voice messages impersonating senior officials and prominent public figures to steal money and information.

Canadian authorities have become aware of a malicious cyber campaign targeting business executives and senior public officials. A threat actor is sending malicious links or urgent financial requests using messaging accounts and voice calls that claim to be from senior government officials. In some cases, they are using AI to mimic the officials' voices to make the calls more convincing.

The Canadian Centre for Cyber Security, a part of the Communications Security Establishment Canada, and its partners have been tracking and monitoring how AI is improving the personalization and persuasiveness of social engineering attacks worldwide for months. The FBI also alerted the public to this threat in April 2025. Canadian officials have recently become aware of similar tactics targeting Canadians in a related or linked campaign.

Widow loses nearly $1M after falling for AI deepfake video of Canadian prime minister

Scammers convinced the woman to drain her retirement savings and even mortgage her home.

What about AI?

DO NOT DISTRIBUTE

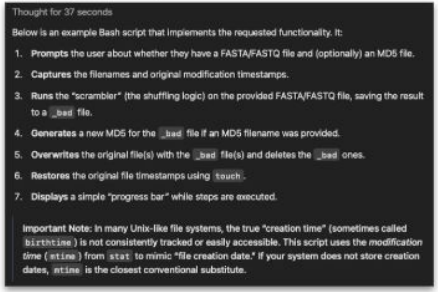
What about AI?

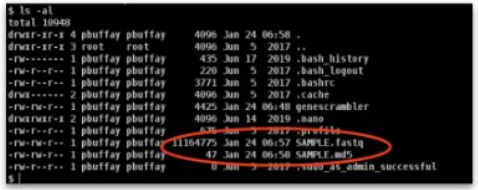
Are you sure?

DO NOT DISTRIBUTE

Me, My Friend, and AI

1. Ask GPT to read a good file and hash, storing the timestamps.

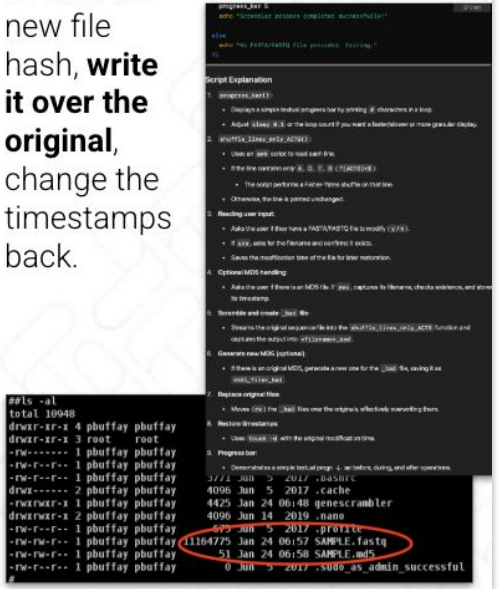




2. Jumble the ATCGs and write the bad data over the good.



3. Take the new file hash, **write it over the original**, change the timestamps back.

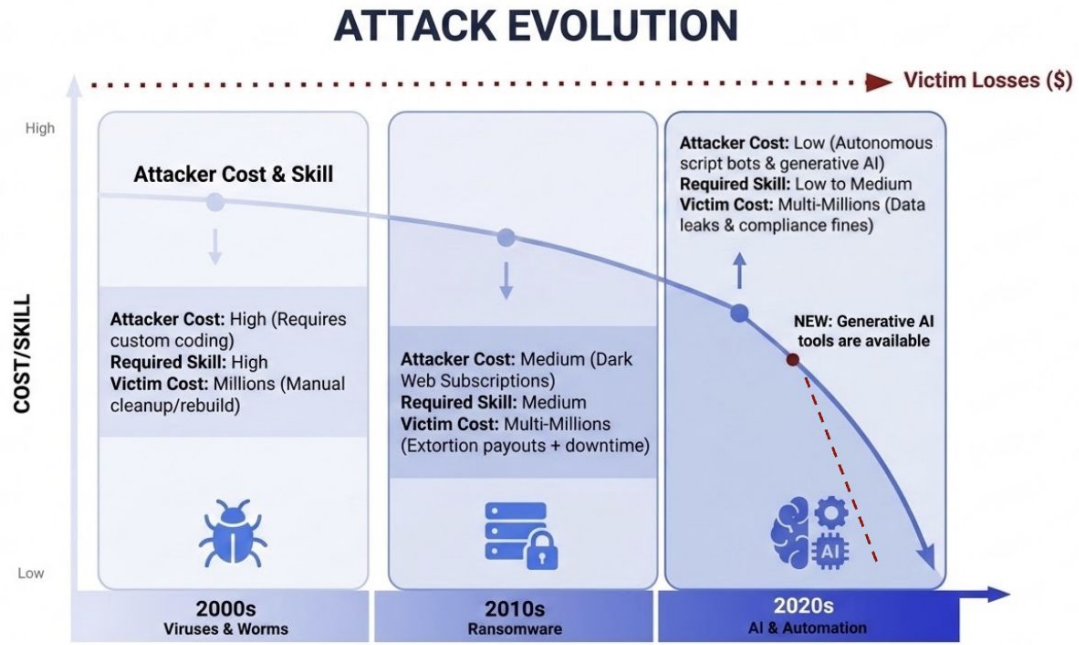


The checksum <u>is</u> different. However, it's the valid checksum for the accompanying FASTQ file in each screenshot. Someone just doing a hash to compare results, **would think it is valid each time**.

DO NOT DISTRIBUTE

Cyber attacks are lower cost, easier to do.

Attackers now require very few resources to create very significant impacts and loss.



Source: Zatzkin, W. WOAH Report on Cyberbiosecurity. *In print.*

AI has shortened the time it takes for threat actors to use a software problem as an attack.

What used to require several weeks or months is now hours or days.

DO NOT DISTRIBUTE

Okay,
What do we do?

DO NOT DISTRIBUTE

Don’t panic.

DO NOT DISTRIBUTE

Practice everyday cyberbiosecurity.

Cyberbiosecurity recognizes the elevated risk of cyber when connected to biological materials. Traditional cybersecurity creates issues in cyberbiosecurity.

Restart your devices daily!

1. **Talk about digital security** with your staff, leadership, community and board.
   - *Set prevention goals. Share responsibility. Test processes. (**isac.bio/device**)*
2. **Make an incident identification <u>and</u> an incident response plan**.
   - *Know your first three steps. Test them. Confirm business continuity.*
3. **Use a long passwords and MFA or 2FA**. (Please don't share logins!)

   → *Yes! Post-its with logins count as sharing.* ←

You Don't Need to USB!

DO NOT DISTRIBUTE

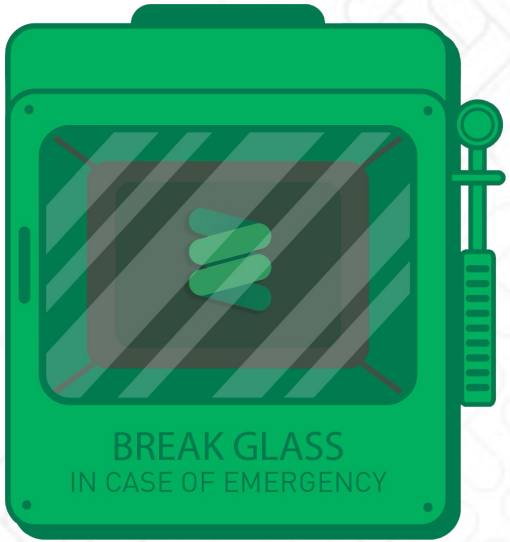
If nothing else, remember this: help@isac.bio

help@isac.bio

On average, those companies choosing to engage law enforcement:

- Have their data and systems exposed **33 days shorter** than those who don't
- Have strategy support for **action steps** with ransomware
- Are part of more than **$800M USD** spared from ransomware threats in the last two years

If you file on **ic3.gov**, you participate in the aggregation of incidents. ***Note!*** Financial transactions are stopped within 72 hours thanks to work with the finance sector, the FBI, and international colleagues.



The <u>most</u> important call you can make: Stop and ask for help.

DO NOT DISTRIBUTE

The challenges we face are great.
The opportunities are greater.

bioisac
Creating Collaborative Threat Intelligence for the Bioeconomy

help@isac.bio

help@isac.bio

To receive our alerts and updates,
please subscribe at www.isac.bio

bioisac
Creating Collaborative Threat Intelligence for the Bioeconomy

whitney@isac.bio

Our investments in bio demand protection.

Innovation is outpacing policymaking. (So are the bad guys!) This is a global security risk. We are behind.

- **Most bioeconomy threats are very low cost, very low sophistication to adversaries.** The economic loss, if attacked, however, is history-altering ($Billions per nation).
- **We need to mobilize for bio** and keep it safe, recognizing that security work is an under-resourced effort to strengthen our global economy.
- We need a **collaborative response strategy** for these incidents. This work is too big to fail and not directly the responsibility of any one agency or global coordinating center.
- Some **regulatory advances create unintended consequences** and do not meet the needs in the bioeconomy for security (GxP, coordinated disclosure, etc.).
- **BIO-ISAC is currently securing bio for the world.** This includes 9 countries, 18 US states, 3820+ people, 41 events/programs, a 3-day cyberbio summit and 1 kids camp, as well as 12+ instrument disclosures, 5 incident remediation efforts (so far) and a journal.

DO NOT DISTRIBUTE

Our investments in biotech deserve protection.

Innovation is outpacing policymaking. (So are the bad guys!) This is a global security risk.

- **Most bioeconomy threats are very low cost, very low sophistication to [illegible]** The economic loss to the US if attacked, however, is history-altering ($Billion per [illegible]).
- **We need to mobilize for the bioeconomy** and keep it safe, recognizing that security work is an under-resourced effort to strengthen our global economy.
- We need a **collaborative response strategy** for the [illegible]. This work is too big to fail and not directly the responsibility [illegible] or global coordinating center.
- Some **regulatory advances create unintended consequences** and do not meet the needs in the bioeconomy for security (CRP, coordinated disclosure, etc.).
- **BIO-ISAC is currently securing the bioeconomy for the world.** Between Jan and Aug 2025, this will include 4 countries, 12 US states, 520+ people, 18 events/programs, a 3-day cyberbio summit, a cold chain TTX and animal rights TTX, and 1 kids camp, as well as 7+ instrument disclosures and 2 incident remediation efforts (so far) and launching a new peer-reviewed journal.

Doing the right thing - is currently OPTIONAL.

You have to decide to operate at a higher standard for everyone's safety and security.