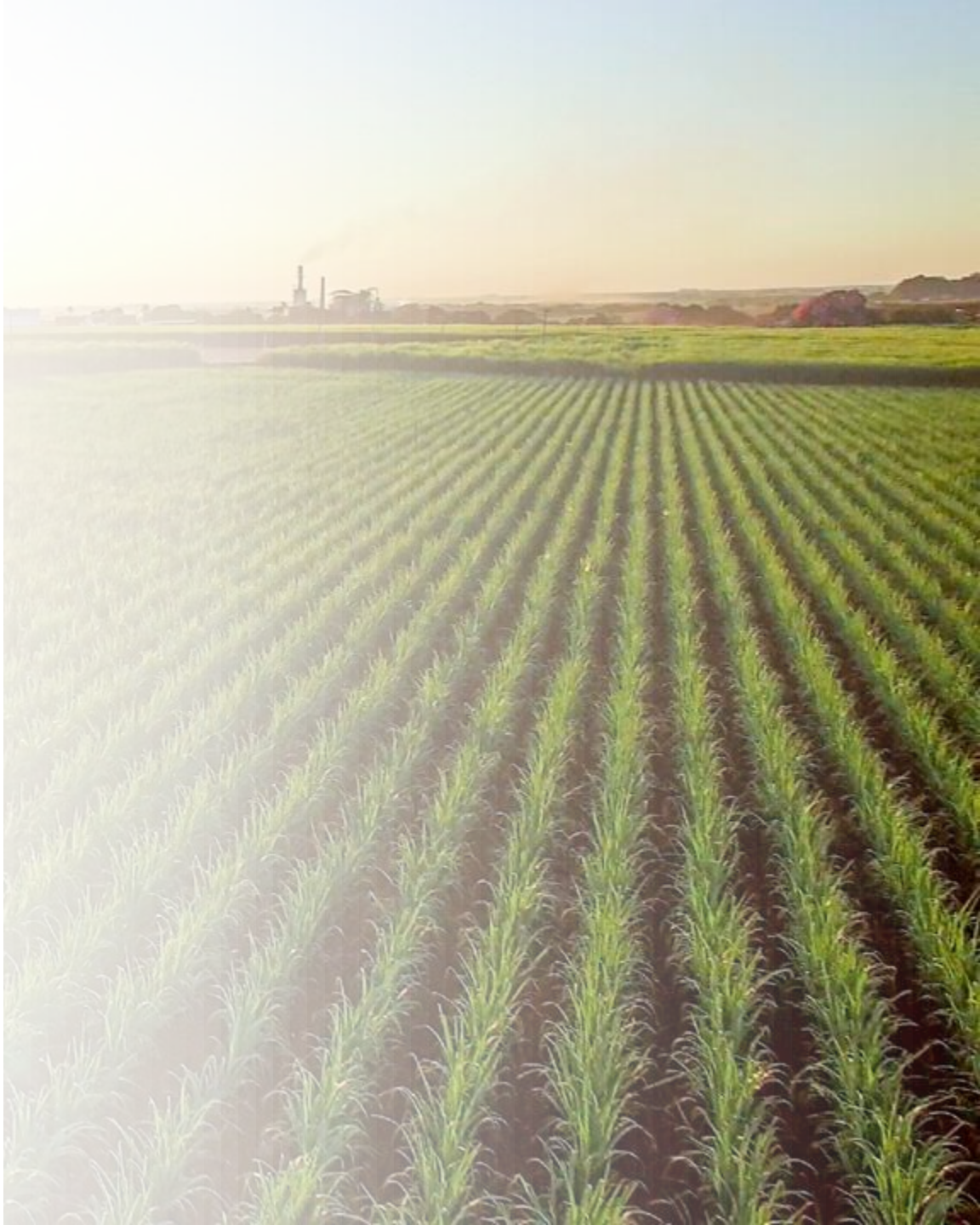
Fielding the Costs:
The Economic Challenges of Staying Secure in the Food and Agriculture Sector

Food Ag ISAC
An IT ISAC Community

October 5, 2024



Food and Ag-ISAC Purpose

The Food and Ag-ISAC is a tailored forum for food and agriculture companies to:

- Engage with leading security experts and analysts from industry peers;
- Share cyber and physical threat intelligence and alerts;
- Drive effective security practices that help detect attacks, respond to incidents, and mitigate risks so they can better protect themselves and the sector; and
- Provide thought leadership to industry, government, and academia.

We are a cost-effective force multiplier for your security teams.

Food Ag ISAC
An IT ISAC Community

The Country's Newest ISAC

- IT-ISAC supported a Special Interest Group (SIG) for food and ag companies since 2013.
- The SIG launched the Food and Ag-ISAC in partnership with the IT-ISAC in May 2023.
- The Food and Ag-ISAC leverages capabilities and analytic resources developed by the IT-ISAC over the past 20+ years.

THE CYBERSECURITY 202

Cyber experts have repeatedly cited the sector's lack of its own ISAC as a dangerous security gap in the industry's ability to get a full picture of the tremendous risks it faces. Backers of the ISAC, which includes major industry players like PepsiCo to Tyson Foods, expect it to fortify the defenses of its members.

- **Tim Stark, The Washington Post Cybersecurity 202**

Food Ag ISAC
An IT ISAC Community

How We Do It

- Mature capabilities - leveraging 23 years experience from the IT-ISAC.
- Adversary Attack Playbooks on hundreds of threat actors.
- Ransomware tracker on thousands of incidents, including those targeting the food and ag industry.
- Threat intelligence platform for automated sharing of indicators.
- Daily, weekly and incident specific, vendor neutral reporting.
- Bi-weekly meetings to discuss threats targeting the industry with peers.
- Engagement with other sectors, the National Council of ISACs, government agencies and academia.

Food Ag ISAC
An IT ISAC Community

Board Members

Food Ag ISAC
An IT ISAC Community

Integration of technology into modern agriculture

=

Increased productivity and larger attack surface

Food Ag ISAC
An IT ISAC Community

Threat Environment Realities

- The attackers are already sharing with each other. They are well-organized, learning from each other, and actively collaborating.
- The threat landscape is too complex for any one company to defend against alone. There are too many threat actors, too many vulnerabilities, and too few resources for any one company to adequately address the threat by itself.
- The economics of cybersecurity favor the attackers. It is more expensive to defend than it is to attack. Defenders need to maximize their resources.

Food Ag ISAC
An IT ISAC Community

Cost to Attack

- Ransomware-as-a-Service (RaaS) can cost as little as $40 per month[1].
- Malware installs per 1,000 vary in cost from $35 for low quality to $4,500+ for high quality[2].
- DDoS attacks vary from $10 - $750[2] based on quality, speed, number of access requests, etc.

Cyber attacks can cost the attackers as low as $40 per month and can return $25,000 per month.

Food Ag ISAC
An IT ISAC Community

Cost of Defending

What organizations spend to protect themselves.

- In 2020, small businesses faced over 700,000 attacks[3] resulting in $2.8 billion in damages.
  - 73% of small businesses[4] reported a cyber incident in 2023
- Global spend on security and risk management is projected to hit **$215 BILLION this year**.
  - 14.3% increase from 2023[5]
- Business on average allocate 10-15%[6] of their annual IT budget to cybersecurity and about $2,700 per full-time employee
- Regulatory and mandatory incident reporting compliance costs increase the cost of defense without any tangible security benefit
- Average data breach cost in 2024 is $4.88 million[7]

It is more expensive to defend than to attack.

Food Ag ISAC
An IT ISAC Community

Cost of Defending - Government

Federal government spends A LOT less on cybersecurity.

- Federal Budget Allocation for cybersecurity in FY2024 is estimated at close to $13 BILLION[8]
  - This is an increase over actual spend in 2023 of $11.19 BILLION but a stark decrease from the spend of over $19 BILLION in 2022.
- CISA FY2024 included $819.3 million[9] for cyber operations
- FBI FY2024 included $90.6 million[10] for cybersecurity expenses.

This number the combined amount outlined for cyber ($63.4m) and cybersecurity ($27.2m) expenses.

Food Ag ISAC
An IT ISAC Community

The Return on Investment

Knowing exactly what threat actors spend on cyber attacks is hard to estimate but we do know that their costs are minimal in comparison to their potentially massive payouts.

- Average ransomware payout cost in 2024 is $2.73 million[11]
- Attackers received more than **$1 billion** in payouts in 2023[12]
- Organizations in the US saw 47% of the world's ransomware attacks[13] in 2023
- Cybersecurity Ventures estimates that global cybercrime will cost $9.5 trillion in 2024 and $10.5 trillion in 2025[14]
  - If "Cybercrime" were a country, it would be the third largest economy in the world[15].

Food Ag ISAC
An IT ISAC Community

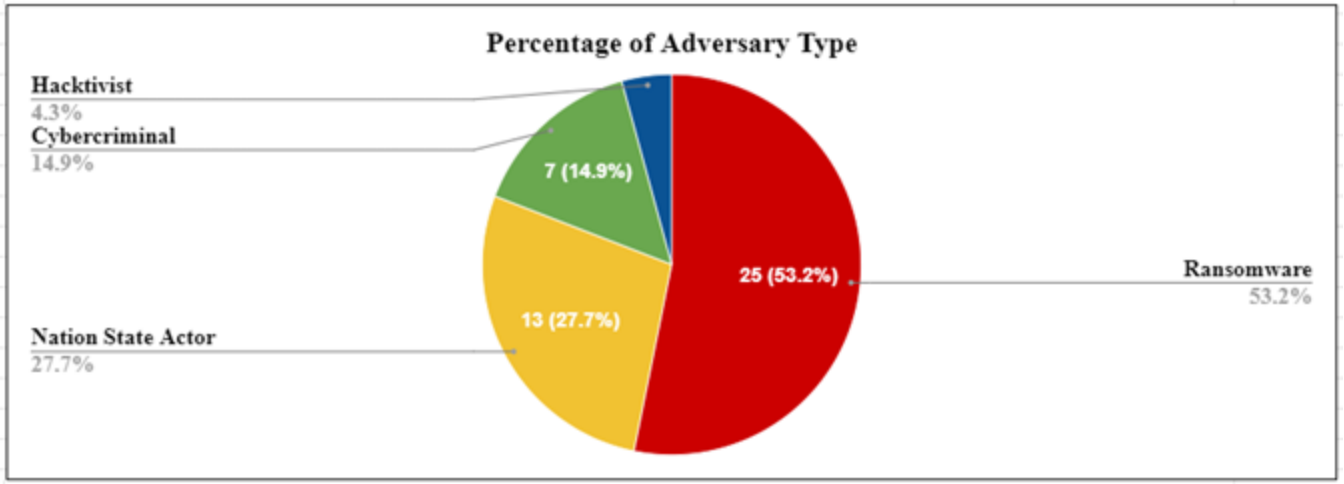
Other Impacts to the Defender

- Evolving and growing threat landscape
  → Sophistication of attacks
  → Increased number of threat actors
- Regulatory compliance and mandatory incident reporting
- Interdependencies and connectedness

Food Ag ISAC
An IT ISAC Community

Threats to the Sector

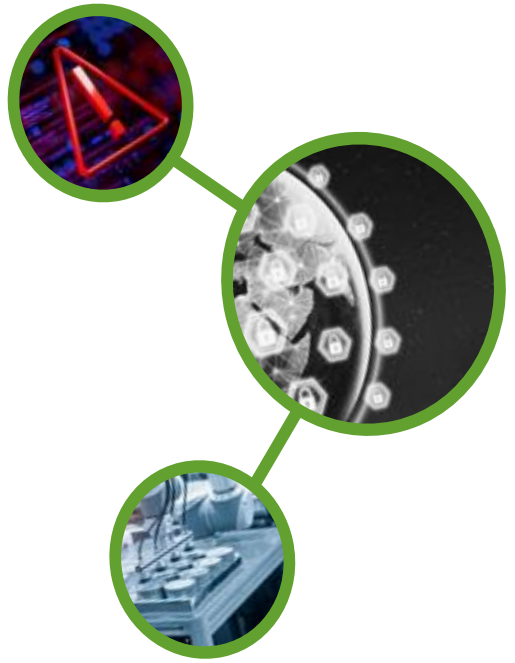
- **Advanced Persistent Threats (APT) Actors**
  Theft of intellectual property and economic data can help foreign nations shortcut their development process, which saves them time and resources.
- **Ransomware**
  Attackers use malware to encrypt files on targeted servers, workstations, industrial controls systems and other essential technologies. Victims are given a ransom demand (typically paid in cryptocurrency) to unlock encrypted files and systems. Double extortion is also common, where threat actors may also leverage the leakage of stolen data to incentivize ransom payments.



Food Ag ISAC
An IT ISAC Community

Advanced Persistent Threat (APT) Actors

- Typically focused on data theft and espionage, especially of data involved in long term developmental intellectual property.
- Theft of this data can help foreign nations shortcut their development process, which saves them time and resources.
- There are a lot of wasted efforts in things like genetic development, and intellectual property can be especially valuable for specific nations.
- APT actors have been known to launch attacks with the goal of disrupting critical infrastructure.
- Several nation states launch cyberattacks against the industry to gain economic advantage.



Food Ag ISAC
An IT ISAC Community

CHINESE CITIZEN'S THEFT OF PROPRIETARY CORN SEEDS TO FULFILL CHINA'S DEVELOPMENT GOALS

A Chinese citizen was sentenced to three years in prison for conspiracy to steal trade secrets from U.S. agriculture companies. The Chinese citizen and five others participated in the theft of inbred corn seeds from fields the companies owned, with the aim of shipping them to a Chinese company. The seeds the Chinese citizen and his co-conspirators targeted were genetically modified to be stronger and enhance desirable traits, such as resistance to pests and drought. The Chinese citizen is assessed to be a non-traditional collector—an individual whose primary profession is not intelligence collection but who collects sensitive U.S. technologies and information on behalf of Chinese government entities.

Developing a single inbred seed can cost

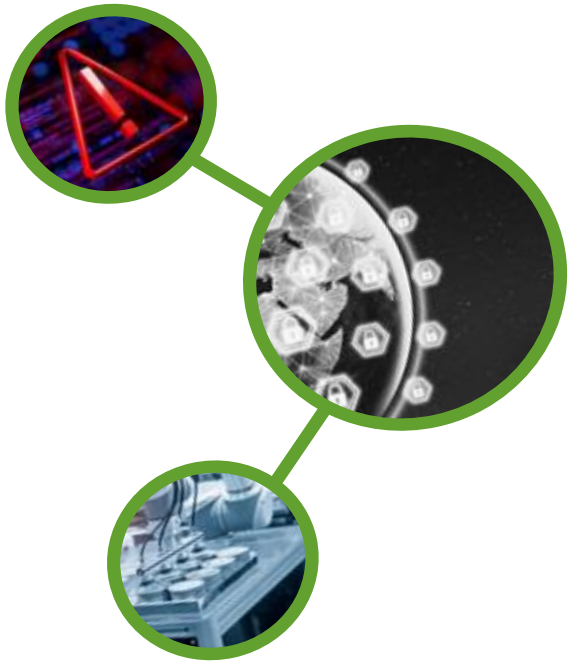
$30–$40 MILLION

in laboratory testing and can take over seven years to develop

The Chinese citizen is also the U.S.-based director of a Chinese company that sold seeds through its subsidiary company. Both companies received favorable treatment from the Chinese government as National Key Dragon Head Enterprises—a designation China bestows on select private companies to recognize the significant role they play in promoting China's modernization and development goals.

A U.S. company informed the FBI it had observed the Chinese citizen digging up corn seeds from one of its farms the previous year. The FBI learned separately a sheriff's deputy had observed the Chinese citizen and two others acting sus-

Advanced Persistent Threat (APT) Actors



Food Ag ISAC
An IT ISAC Community

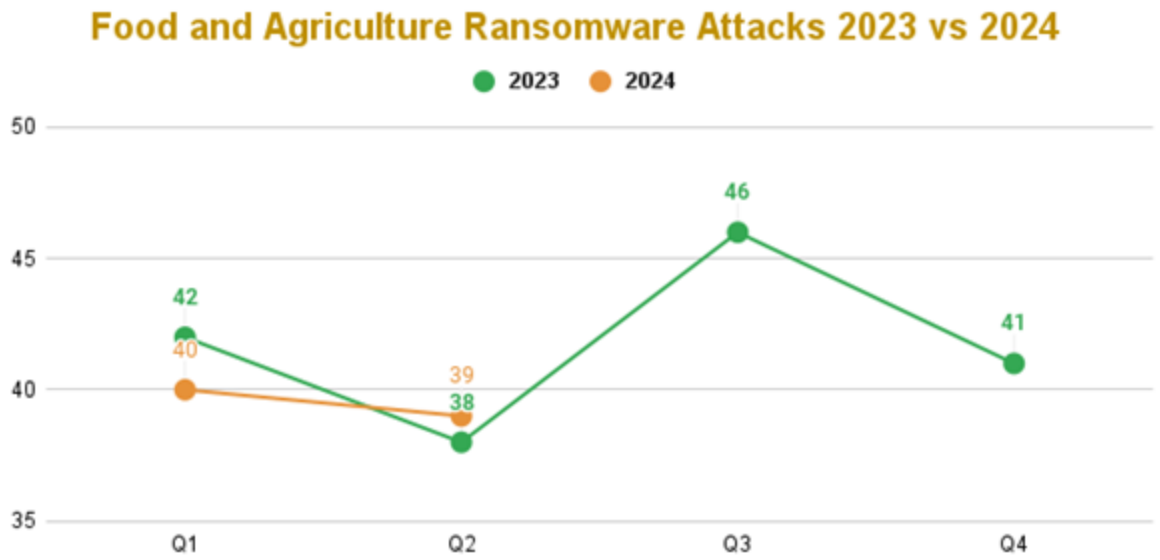
Ransomware

- Since 2020 we have tracked over 6,500 ransomware incidents.
- In 2023, the IT-ISAC and the Food and Ag-ISAC tracked 3,006 total ransomware incidents.
  - **167** of these were against the food and agriculture sector, which accounted for **5.5%** by volume of total attacks.
- Ransomware is especially impactful for the food and ag sector:
  - Just-in-time delivery of essential products
  - Impacts to human health and safety
  - Theft of sensitive intellectual property
  - Vulnerable to cross sector impacts (Water, Oil and Natural Gas, Transportation, Communications)
  - Vulnerable supply chain who may not have mature cybersecurity capabilities

Food Ag ISAC
An IT ISAC Community

Ransomware - 2024 Update

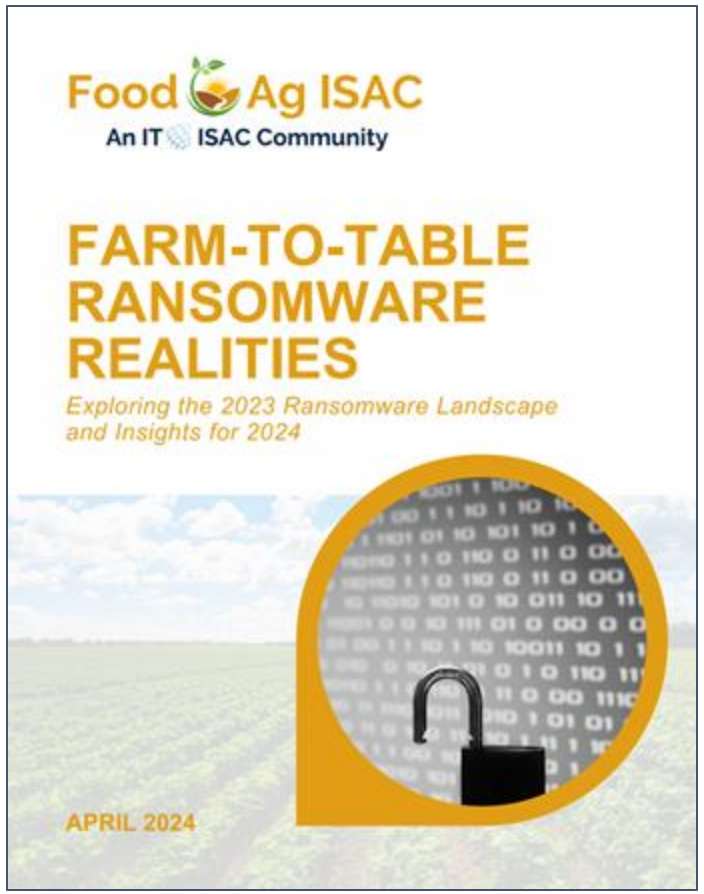
- In 2024 (Q1 and Q2), we have tracked over **1,000 ransomware attacks** across all sectors.
- **80 of these attacks** have been attributed to the food and ag sector, which accounts for around 7% of the total targeting.

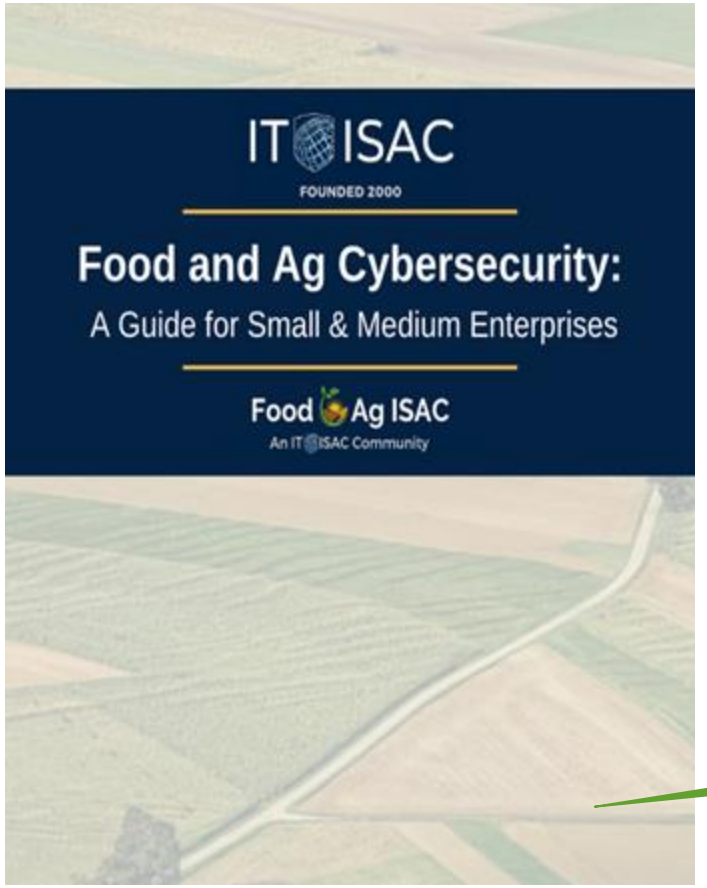


Food and Ag-ISAC Ransomware Dashboard Q1-Q2 2024

Food Ag ISAC
An IT ISAC Community

Resources





Visit FoodAndAg-ISAC.org to tap into resources like our **Ransomware Report** and **Cybersecurity Guide for Small & Medium Enterprises**.

Check out FoodAndAg-ISAC.org!

Food Ag ISAC
An IT ISAC Community

Be a Force Multiplier

→ We defend better when we defend together.

→ Leverage resources and capabilities of peer companies to maximize your security spend.

→ Voluntary action will drive better and more cost effective outcomes than government regulations.

Food Ag ISAC
An IT ISAC Community

Thank You!

Scott@FoodandAg-ISAC.org

FoodandAg-ISAC.org

Food Ag ISAC

An IT ISAC Community

References

1. https://www.rapid7.com/blog/post/2023/08/22/ransomware-as-a-service-cheat-sheet/
2. https://www.privacyaffairs.com/dark-web-price-index-2023/
3. https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/
4. https://www.idtheftcenter.org/post/2023-business-impact-report-record-level-attacks-still-high-confidence-in-defense/
5. https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024
6. https://www2.deloitte.com/content/dam/insights/us/articles/6507_Cybersecurity-FS-ISAC/DI_2020-FS-ISAC-Cybersecurity.pdf
7. https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf
8. https://www.statista.com/statistics/675399/us-government-spending-cyber-security/
9. https://www.meritalk.com/articles/cisa-taking-34m-budget-slash-for-fy2024/
10. https://www.justice.gov/d9/2023-03/fbi_fy_24_pb_bud_sum_ii_omb_cleared_3-08-23.pdf
11. https://www.varonis.com/blog/ransomware-statistics#:~:text=The%20average%20ransom%20in%202024,(NetApp)
12. https://www.wired.com/story/state-of-ransomware-2024/
13. https://aag-it.com/the-latest-ransomware-statistics/
14. https://www.cysuranceinstitute.com/insights/report-cybercrime-to-cost-the-world-95-trillion-usd-annually-in-2024-according-to-cybersecurity-venture
15. https://www.usnews.com/news/best-countries/articles/the-top-10-economies-in-the-world

Food Ag ISAC
An IT ISAC Community