

## Draft Pending Adoption

Attachment 1  
Cybersecurity (H) Working Group  
7/9/24

Draft: 6/17/24

### Cybersecurity (H) Working Group Virtual Meeting May 20, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met May 20, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Julia Jette (AK); Bud Leiner (AZ); Wanchin Chou (CT); Tim Li (DE); Tia Taylor (GA); Lance Hirano (HI); Daniel Mathis (IA); C.J. Metcalf (IL); Mary Kwei (MD); Jake Martin (MI); Bubba Aguirre (MN); Tracy Biehn (NC); Colton Schulz (ND); Christian Citarella (NH); Scott Kipper (NV); Gille Ann Rabbin (NY); Matt Walsh (OH); David Buono (PA); John Haworth (WA); Rebecca Rebholz (WI); and Lela Ladd (WY).

#### 1. Heard an Update on the CERP

Peterson provided a brief update on the Cybersecurity Event Response Plan (CERP), which was adopted at the Spring National Meeting. To add background for those who need it, Peterson said the CERP is meant to assist states with implementing their own versions of the *Insurance Data Security Model Law* (#668). The long-term goal of the CERP is to act as a living document that can be updated over time to achieve convergence in the cybersecurity event response space.

Peterson discussed the difficulties included in various notification laws: Multiple departments require similar types of data to be included, but the reporting method and updating vary. The added complications are not helpful during an already stressful time. After multiple discussions, the direction is leaning toward a confidential repository at the NAIC. Additionally, similar solutions have been utilized for licensee filings of risk-based capital (RBC), Market Conduct Annual Statement (MCAS), as well as System for Electronic Rates & Forms Filing (SERFF) confidential and trade secrets filings. This type of repository would offer improved security, heightened awareness, and more confidential treatment.

Peterson stated there remains a lot of work to do, but the intent is to get a lot of agreement on this particular project and for it to be viewed as an improvement that will benefit supervisors and licensees alike.

#### 2. Heard a Presentation from CyberCube on Cyber Risk

Amann introduced Rebecca Bole (CyberCube) and Jon Laux (CyberCube), emphasizing their cybersecurity and insurance expertise.

Bole offered the presentation as an opportunity for reflection on data, methods available, and what is being used in the insurance industry. Namely, she said she would discuss what is happening in the cyber risk landscape and how it is applied to insurance, focusing on the cyber risk the insurance industry takes.

CyberCube is a data analytics company seeking to provide analytics to quantify cyber risk for its clients. CyberCube partners with state insurance regulators, rating agencies, and government agencies to create frameworks for governance. Bole cited the company's active partnership with the U.S. Department of the Treasury (Treasury Department) as the Federal Insurance Office (FIO) seeks to understand catastrophic cyber risk in the U.S. economy to structure appropriate federal responses.

## Draft Pending Adoption

Attachment 1  
Cybersecurity (H) Working Group  
7/9/24

Laux presented a brief, high-level overview of the state of the cyber market, adding additional context to describe cyber risk at a conceptual level, such as in property/casualty (P/C) and terrorism. Observations indicate cyber insurance is among the most volatile P/C lines of business.

When asked to talk about the data available for underwriting, Laux said the good and bad news is that cyber risk data is everywhere. He said everything digital is tracked in a way the physical world is not. This can be frightening from a privacy point of view, but from a data point of view, there is a lot to look at. Laux said that, broadly, many underwriters are trying to use a combination of external and internal network scans. Utilizing information, they can scan a network with tools from CyberCube, SecurityScorecard, or Bitsight. Scalable intelligence can be done to look at organizations in many of the same ways those with ill intent do. If those with ill intent can see that a particular technology vulnerability is open, that is the first step in exploiting it. While challenging, there are some places this can be done. In practice, a lot of the information is obtained through underwriting questionnaires to fill in the gaps.

Laux said an important and relevant question is whether we can use the data quickly and efficiently and make sense of what trends might be coming in. Detailed analysis can inform decision-making and quantify the importance of security signals. He said CyberCube carefully reviews 40 different information signals that indicate an organization's risk posture. Once digested, the organization is given a security score of 0–100. Laux pointed out the presence of things one might call “negative hygiene,” sort of the equivalent of leaving your doors unlocked if you are in an unsafe neighborhood, and everything on the internet is potentially an unsafe neighborhood. Those are important because they are signals that, while indicative that things are problematic for the organization, can be avoided. For instance, ports can be closed, and software updates can be deployed to resolve the issue. Laux stated the level of accumulation risk has grown significantly for the industry. CyberCube sees a cutting edge around the point of underwriting, looking at the marginal risk of any given policy. An organization can look at a point of underwriting, what each policy they are considering bringing on to their books does to their overall tail exposure.

Without clear public sector direction from state insurance regulators or any other group, the markets have been grappling with the challenge of knowing when things have become too big. Similar to how terrorism was kicked out of property policies after the Sept. 11, 2001 terrorist attacks, insurers are afraid of something comparable happening in the digital space. Various approaches to addressing the question have been observed through exclusions, much like critical infrastructure is often excluded. Carriers are also evaluating widespread event triggers or limits, similar to how hurricane is done. Some insurers are exploring sub-limits to contain some of their tail risk. Mitigation potential can be further extended through active risk monitoring. Developing alerts and notifications or sending additional questions to a policyholder allows for assessing where their exposures are and knowing how they are adapting to these things.

Laux offered three final points: 1) cyber insurance requires adaptiveness and ongoing engagement with policyholders to improve resilience and reduce potential claim costs; 2) there is an abundance of data available to cyber insurers for underwriting and risk management; and 3) understanding an insurer's use of data, level of testing, and adaptability to change are important criteria for underwriting maturity.

Bruce Jenson (NAIC) asked about cyber catastrophe bond issuance, particularly whether CyberCube expects more activity in this space. Laux observed four catastrophe bonds issued before Jan. 1 of this year. CyberCube was the lead modeler for three and was also highly involved in the fourth. Laux said CyberCube does think the market could adopt this. This first issue cycle was just the beginning. He said that, in many ways, CyberCube hopes this becomes a robust cap bond support for cyberspace. Bole suggested that the injection of capital markets capital

## Draft Pending Adoption

Attachment 1  
Cybersecurity (H) Working Group  
7/9/24

and due diligence into the cyber insurance and reinsurance market is a real test and, ultimately, validation of the market's maturity. There is a high level of due diligence in the transactions, not just modeling, but the coverage, definitions, and clarity of exposure the bonds take on. This capital source is a strong positive indicator of the growth of this market.

Peterson posed a series of questions. Firstly, he asked who the typical buyer of cyber insurance is. He then asked if most buyers are relatively sophisticated businesses or if they are individuals also purchasing cyber insurance. Lastly, Peterson asked whether we expect the current buyer demographic to continue into the future. Laux answered by saying the typical buyer is an American business. Recognizing the product's rapid growth in other parts of the world, the U.S. has had the deepest penetration for insurance buyers. He provided additional observations of the largest companies beginning to purchase cyber insurance policies as far back as 2004, when privacy laws were first put in place. He said today's market has expanded to include the small business world following the ransomware trends. Based on the NAIC's own data, Laux reflected on an area of continued development between companies buying standalone cyber insurance policies and companies purchasing an endorsement of some kind.

Regarding the current mix of buyers, Laux suggested it would not be surprising to see more small organizations buying standalone insurance coverage over time, where it is efficient for the company. Individuals purchasing cyber insurance are likely to continue to be high-net-worth individuals with concerns of having something to potentially lose.

Amann offered appreciation for Bole and Laux's expertise and extended an offer for them to return for a future presentation. She also suggested the audience should expect an email regarding the CERP and provide ideas and suggestions for other speakers to participate in the Working Group's charge to provide cybersecurity and cyber insurance education.

Having no further business, the Cybersecurity (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024\_Summer/WG-Cybersecurity/Minutes-CyberWG052024.docx

## Draft Pending Adoption

Attachment 1  
Cybersecurity (H) Working Group  
7/9/24

Draft: 4/16/24

### Cybersecurity (H) Working Group Virtual Meeting March 27, 2024

The Cybersecurity (H) Working Group met March 27, 2024. The following Working Group members participated: Cynthia Amann, Chair, and Brad Gerling (MO); Michael Peterson, Vice Chair (VA); Julia Jette (AK); Chris Erwin (AR); Bud Leiner (AZ); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Elizabeth Nunes (GA); Daniel Mathis (IA); C.J. Metcalf (IL); Shane Mead (KS); Mary Kwei (MD); Jake Martin (MI); T.J. Patton (MN); Tracy Biehn (NC); Martin Swanson (NE); Colton Schulz (ND); Christian Citarella (NH); Nick Stosic (NV); Gille Ann Rabbin (NY); Don Layson and Matt Walsh (OH); David Buono (PA); John Haworth (WA); Andrea Davenport (WI); and Lela Ladd (WY).

#### 1. Heard an Update on White House ONCD Activities Related to Cybersecurity and Cyber Insurance

Amann introduced Stephen Viña, Senior Advisor with the Office of the National Cyber Director (ONCD) of the White House. Viña noted that the ONCD helps monitor threats and coordinate responses.

Viña provided an overview of the ONCD's activities, including a briefing on the contents and intent of the National Cybersecurity Strategy.

Viña noted that the development of the National Cybersecurity Strategy included consultations with interagency and external stakeholders and built on previous strategies, including President Biden's work of the prior two years. The goal is to have a digital ecosystem that is more inherently defensible and resilient.

Viña said the strategy represents a fundamental shift in rebalancing the responsibility to defend cyberspace and realigning incentives to favor long-term investments. The National Cybersecurity Strategy is organized around five pillars, which include: 1) defending critical infrastructure; 2) disrupting and dismantling threat actors 3) shaping market forces to drive security and resilience; 4) investing in a resilient future; and 5) forging international partnerships.

The ONCD published an implementation plan July 13, 2023, including 69 initiatives, each with a singular, responsible agency and a completion date. The expectation is that the implementation plan will be updated at least annually, with the ONCD reporting on the progress and effectiveness of the strategy.

Viña then provided an update on other initiatives, including discussions that the ONCD is engaging in to encourage harmonization of cybersecurity standards and the ONCD/U.S. Department of the Treasury (Treasury Department's) continued study of the possibility of a cyber insurance federal backstop. Related to the federal backstop, Viña that the Treasury Department had issued a request for input in 2023 and is currently studying responses, including considering what a federal backstop would cover, whether it would be mandatory, and what would trigger the backstop. Viña noted that the Treasury Department will host a Spring Symposium to continue the discussion and study of the matter.

Regarding ransomware, Viña noted that the ONCD has observed that ransomware payments have become less common but more severe, indicating that threat actors are "big game hunting," seeking larger payouts for their activities. Ultimately, he said that the federal government strongly discourages payments and that ransom payments should be a last resort to avoid encouraging continued activity by threat actors.

## Draft Pending Adoption

Attachment 1  
Cybersecurity (H) Working Group  
7/9/24

Lastly, Viña referred to the ongoing discussions regarding the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA), which may impact insurers depending on the final determination of who is considered to be critical infrastructure.

Amann transitioned to the question-and-answer portion of the discussion, which began with a question from Chou. Chou asked about consumer perspectives on the ONCD's activity and consumer awareness of their use of data, particularly with regard to automobile monitoring/use of consumer data, including how to communicate with consumers. Viña noted that the ONCD was not going to work on cyber incident reporting as other agencies would address that via their own rulemaking process.

Romero asked about the timeline for the backstop discussions. Viña said the Treasury Department responded that its conference in the spring is the next meaningful milestone and suggested the Working Group connect with Steven Seize (Treasury Department) for additional information.

Amann asked about the significance of legacy systems as a root cause for cybersecurity events and how to encourage better recognition of the security threat legacy systems can represent. Amann also suggested that better underwriting practices could encourage better risk hygiene to, in turn, prevent more security incidents from occurring. Viña acknowledged the importance of the legacy systems discussion and pointed to the ONCD's work encouraging long-term investments because, with legacy systems, manufacturer support has typically ended; thus, security updates are no longer available, leading to increasingly vulnerable infrastructure.

Viña also introduced Jeff Rothblum (ONCD) as a colleague who will engage in cyber insurance matters going forward.

### 2. Discussed Other Matters

Peterson provided a brief update, noting that now that the Cybersecurity Event Response Plan (CERP) has been adopted, the next discussion will be about taking cyber event notifications safely and securely.

Having no further business, the Cybersecurity (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024\_Spring/WG-Cybersecurity/Minutes-CyberWG031724-Final.docx

## Draft Pending Adoption

Attachment 1  
Cybersecurity (H) Working Group  
7/9/24

Draft: 4/2/24

Cybersecurity (H) Working Group  
Phoenix, AZ  
March 17, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Phoenix, AZ, March 17, 2024. The following Working Group members participated: Cynthia Amann, Chair, and Brad Gerling (MO); Michael Peterson, Vice Chair (VA); Chris Erwin (AR); Wanchin Chou (CT); Daniel Mathis (IA); Ryan Gillespie and Erica Weyhenmeyer (IL); Craig VanAalst (KS); Kory Boone (MD); Jeff Hayden (MI); T.J. Patton (MN); Colton Schulz (ND); Christian Citarella (NH); David Cassetty and Nick Stosic (NV); Avani Shah/Sumit Sud (NY); Matt Walsh (OH); John Haworth (WA); and Tim Cornelius and Rebecca Rebholz (WI). Also participating was: David Buono (PA).

### 1. Adopted its 2023 Fall National Meeting Minutes

Haworth made a motion, seconded by Peterson, to adopt the Working Group's Nov. 16, 2023, minutes. (*see NAIC Proceedings – Fall 2023, Cybersecurity Insurance (H) Working Group, Attachment Three*). The motion passed unanimously.

### 2. Adopted the Cybersecurity Event Response Plan (CERP)

Amann recognized Peterson for spearheading the Cybersecurity Event Response Plan (CERP) and Rabin for working with Peterson on the document. She said the CERP is intended to be guidance for departments of insurance (DOIs) when they must respond to a cybersecurity event. The plan will also help new DOI employees understand the response process. If a state has adopted its own version of the NAIC *Insurance Data Security Model Law* (#668), the information in the guidance will need to be updated to comply with the state's law. Additionally, states can change the document information to meet their needs. The document includes topics such as communication among various stakeholders, understanding and receiving notifications, required information that needs to be provided to a DOI, and a process that can be used to respond to cybersecurity events defined in the Model #668. The document also includes a sample template that can be used by a DOI when requesting information from the breached party. The Working Group worked closely with interested parties to incorporate their suggestions into the CERP. The document was exposed twice, and suggested changes were made where applicable.

Peterson made a motion, seconded by Haworth, to adopt the CERP (Attachment Two-A). The motion passed unanimously.

### 3. Heard a Presentation from the Academy on its Cyber-Risk Activities

Richard Gibson (American Academy of Actuaries—Academy) gave an informational presentation to the Working Group. The Academy is the only U.S.-based actuarial organization solely focused on serving the public and the entire actuarial profession. The Academy encompasses all practice areas and ensures the profession's ability to self-regulate by housing the actual board for counseling and disciplining, the joint committee on the code of professional conduct, and the committee on qualifications. Chou is the chairperson of the committee on cyber risk.

## Draft Pending Adoption

Attachment 1  
Cybersecurity (H) Working Group  
7/9/24

The Academy is engaged in public policy issues. The Academy's Casualty Practice Council (CPC) is the umbrella committee for major property/casualty (P/C) insurance issues. The CPC provides objective technical expertise to policymakers and regulators. The Academy does not work for insurers or regulators. The Academy has a committee on cyber risk that monitors the actual aspects of cyber risk. There are more than 20 members on this team, all of which are volunteers. A majority of the volunteers on the committee are working in cyber on a regular basis.

The Academy has been working on a cyber risk toolkit for the last three to four years and continues to update the toolkit on a regular basis. The toolkit includes papers that address issues pertinent to cyber risk and exposures that are now impacting most lines of business. Cyber exposure extends to many other coverages. Each part of the toolkit is a standalone paper, but it provides a cohesive overview of the challenges posed in the cyber insurance market. The cyber insurance market is constantly evolving with respect to new threats, new coverages, and new crises. The toolkit will be updated periodically to reflect new and emerging work from the Cyber Risk Committee.

The key papers within the Cyber Risk Toolkit include *An Introduction to Cyber; Cyber Threat Landscape; Silent Cyber; Cyber Data; Cyber Risk Accumulation; Cyber Risk Reinsurance Issues; Ransomware; War, Cyberterrorism, and Cyber Insurance; Autonomous Vehicles and Cyber Risk; Personal Cyber: An Intro to Risk Reduction and Mitigation Strategies; Digital Assets and Their Current Roles Within Cyber Crime; and Cyber Risk Resource Guide.*

The Cyber Risk Committee is currently in the process of a cyber vendor model review. While the committee is not able to review all of the existing cyber models, it is trying to get a sense of how cyber models are working and how they are evolving. The Academy is not endorsing models but trying to understand the parameters and the output they provide, as well as the model's usefulness.

The Cyber Risk Committee is also working on an outline for international cyber considerations and delving deeper into cyber personal lines insurance and the rating on the personal lines side of cyber insurance. An outline about cyber insurance and directors and officers (D&O) coverage is also in the works. In 2020, the Academy published a report on cyber breach reporting requirements, which provides an analysis of laws across the U.S. This document can be found on the Academy's website.

The Academy is working with a business school in Paris, France, to estimate the economic value of cyber risk. The methods being used consider both the heavy-tailed distribution of extreme events and the rapid changes in the underlying hazard. The hope is to get access to the Federal Bureau of Investigation's (FBI's) database on cyber events so work can move forward and be reproduced for the U.S. The Working Group will continue its interaction with the Academy.

#### 4. Heard a Presentation from CyberAcuView About its Organization

Monica Lindeen (CyberAcuView) said the cyber-insurance market continues to mature. Following a health care data breach in 2015, the cyber-insurance market began to harden. In 2016 and 2017, a lot of new carriers entered the cyber-insurance market, and coverage began expanding. While 2018 and 2019 saw lower rates, ransomware severity increased.

CyberAcuView was created by insurance industry leaders, and the organization acts as a thought leader on issues surrounding cyber insurance. CyberAcuView was formed to help increase innovation and competition in the cyber-insurance market and to help combat the increasing threat of cyberattacks. Since CyberAcuView's establishment, it has been working to help insurers provide better value and service to its policyholders and their cyber-risk

mitigation. The organization also has been helping to provide leadership in fighting cybercrime to improve resilience to cyber risk, as well as helping to ensure a competitive cyber-insurance market. CyberAcuView believes the cyber-insurance market will continue to mature with access to experience data, stronger underwriting, capital market investments, the development of cyber definitions and standards, engagement with law enforcement, and collaboration of systemic resolutions that will benefit both the policyholders and society.

Mark Camillo (CyberAcuView) said the core reason for CyberAcuView being formed was data aggregation. There are currently more than 20 members that participate in CyberAcuView, which represents approximately 60% of the cyber-insurance market. However, not everyone in the market reports data. Prior to the formation of CyberAcuView, there was not a platform that insurers had to benchmark how they were performing against their peers and how their loss ratios were looking in various industries and segments. CyberAcuView began to collect and aggregate data. CyberAcuView's collection of the data and aggregation provides a benchmark to insurers. On a quarterly basis, claims data is aggregated, anonymized, and provided to CyberAcuView's members. To get data out of the pool, the insurer must provide data, as the data services are voluntary. CyberAcuView enables insurers to retain the value of their own data by being a statistical reporting agent. Statistical reporting services are available in all states, as required.

CyberAcuView is also working on cyber-data standards. It developed an incident response claims taxonomy for both cyber exposures and cyber claims data. CyberAcuView also publishes standards as an open cyber standard that is governed by CyberAcuView and can be accessed and used by all market participants. CyberAcuView has started collecting data in 2019 and has data through the end of the third quarter of 2023. Over 30,000 claims have come in since 2019, and a little over \$4 billion in payments, with about \$500 million in reserves. Less than one-third of the claims are for ransomware. However, more than half of those losses were actually caused or driven by ransomware. CyberAcuView collects the top ransomware variants in terms of ransomware claims. It also provides information about the industry groups and tracks the number of claims notices.

CyberAcuView runs quarterly workshops to stimulate discussion and help insurers develop a better understanding of events that drive systemic risk. They also discuss how insurers can help the areas of systemic risk, and how to help increase society's resilience to systemic cyber risk. Past workshops have focused on cloud failure and outages, issues confronting cyber insurance-linked securities (ILS)/alternative capital markets, systemic risk extensions that have been introduced in the marketplace, and cyber risk modeling considerations.

Lindeen leads the efforts on regulatory collaboration, acting as a resource for organizations.

Camillo addressed the potential federal cyber backstop. CyberAcuView will continue to evaluate the potential of a federal cyber backstop.

CyberAcuView has a head of law enforcement engagement that works closely with the FBI through its public/private partnership with the National Cyber-Forensics and Training Alliance (NCFTA). The group is developing a pilot program to actively disrupt and seize ransomware payments by coordinating with other technology companies.

CyberAcuView developed a policy form that can be used by market participants to define risks more precisely, remove ambiguities, and attract more capacity into the market. The cyber war exclusion language was accepted and posted to the Legal Marketing Association (LMA) website. Several insurers are currently going through the process of updating their war language and using the CyberAcuView war exclusion language as a template.



## Draft Pending Adoption

Attachment 1  
Cybersecurity (H) Working Group  
7/9/24

CyberAcuView has endorsed the Cybersecurity and Infrastructure Security Agency's (CISA's) bad practices list as a voluntary minimum cybersecurity best practice to improve policyholder security maturity. It also has expanded outside of the U.S., with its first international data call in the United Kingdom (UK) and Canada.

CyberAcuView collaborated with Pan-European Insurance Risks Information System (PERILS) in Europe to create a U.S. cyber loss index to help accelerate the growth of the cyber ILS and industry loss warranty (ILW) markets. PERILS does work similar to CyberAcuView for the European market on the natural catastrophe side.

The only 2023 event CyberAcuView continues to track is the MOVEit vulnerability. Based on the data they were able to gather and collect in the first quarter of 2024, the losses are below the \$500 million reporting threshold. CyberAcuView will continue to monitor to see if the cost rises above the threshold. The methodology can be found by visiting <https://cyber.perils.org/#methodology>.

### 5. Discussed the Working Group's Work Plan

The Working Group will look at the current *Cybersecurity Supplement* to see what other information might be advantageous to collect. The Working Group also will discuss some of the following issues in the next year:

- The impact of both hardware and software legacy systems.
- Reviewing the European Union's (EU's) recent Artificial Intelligence Act to the extent that it impacts cyber.
- Data modernization and standardization.
- Third-party vendor oversight.
- Educating its fellow regulators and the insurance industry.
- The knowledge among regulators regarding cyber is disparate, so the Working Group will make sure information is being brought to it from experts.
- Two panels at the Insurance Summit.
- One-to-many reporting.
- Ensuring that both small and large businesses are aware of what their cyber coverage actually covers.
- Working with the Information Technology (IT) Examination (E) Working Group.
- Tracking Model #668 adoptions, as well as changes by the states adopting the model law.
- Panels with an insurer, broker, and reinsurer.
- Hearing from the Center for Insurance Policy and Research (CIPR).
- Hearing from CyberCube.

Peterson is a member of the Financial Stability Board (FSB) for discussions about cybersecurity event notifications standardization.

### 6. Discussed Other Matters

Amann reminded the Working Group of the Working Group's call on March 27.

Having no further business, the Cybersecurity (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024\_Spring/WG-Cybersecurity/Minutes-CyberWG031724-Final.docx

# The Changing Landscape of Cyber Threats

July 9, 2024

# Examples of What is Being Targeted

- Bulk PII, PHI, PCI
  - Criminal, CI targeting
  - OPM, Healthcare/Insurance, Bank/Finance, Data Aggregators, Credit Card Cos.
- Medical
  - Economic
  - Universities, pharma, medical device and research companies
- Agriculture
  - Economic
  - Universities, Bioengineering, Research
- IoT
  - Economic
  - New, vulnerable platforms - Vehicle Industry, Research firms.
- Trusted vendors
  - Small business, contractors Third party systems (software, hardware) connected to your systems
  - Law firms, auditing firms

# Type of Attacks

- **Ransomware and Extortion**
- **Business E-mail Compromise**
- Website Defacements
- **Investment Scams**
- False Tax Return Filings
- **Tech Support**
- Theft of PII, PHI
- Theft of IP
- DDoS
- Point of Sale Breaches
- Phishing

# Ransomware

## WHAT IS RANSOMWARE?

A form of malware that encrypts files on a victim's computer or server, making them unusable. Cyber criminals demand a ransom in exchange for providing a key to decrypt the victim's files.

Ransomware attacks are **becoming more targeted, sophisticated, and costly**, even as the overall frequency of attacks remains consistent. *Since 2018, broad, indiscriminate* ransomware campaigns have declined, but the losses from ransomware attacks have increased, according to complaints received by IC3 and FBI case information.

Expected targets of ransomware like state and local governments continue to occur, ransomware actors have **aggressively targeted** health care organizations, industrial companies, and the transportation sector.

## RANSOMWARE INFECTION?

Cyber criminals use a variety of techniques to infect victim systems with ransomware. Cyber criminals upgrade and change their techniques to make their attacks more effective and to prevent detection.

**Infection Vectors**: Email phishing campaigns, Remote Desktop Protocol vulnerabilities, & Software vulnerabilities. (avenues of infection: Third Parties and Managed Service Providers.)

# Implications of Ransomware

In **2023**, the FBI Internet Crime Complaint Center (IC3) received **over 2,800** complaints identified as ransomware with adjusted losses of approximately **\$60 million**.

This report only refers to the complaints filed to the IC3 and not directly to FBI agents or offices. Therefore, the actual cost and the number of attacks are probably much higher.

## **Paying the ransom won't stop future attacks**

"Separate studies have shown **50-80 percent** of **victims** that paid the ransom experienced a repeat ransomware attack by either the same or different actors"

# Ransomware – Best Practices

## CYBER DEFENSE BEST PRACTICES

- **Regularly back up data and verify its integrity.** Backup should be isolated from network.
- Focus on **awareness** and **training**.
- Patch the OS, software, and firmware on devices. Patch all endpoints as vulnerabilities are discovered.
- Ensure **anti-virus** and **anti-malware** solutions are set to **automatically update** and conduct **regular scans**.
- Implement the “**least privilege**” for file, directory, network share permissions and configure access controls.
- Disable macro scripts from Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office Suite applications.
- **Implement software restriction policies** or other **controls** to prevent program execution in common ransomware locations.
- Employ best practices for use of **Remote Desktop Protocol (RDP)**, including auditing your network for systems using RDP, closing unused RDP ports, applying two-factor authentication, and logging RDP login attempts.
- Implement application **whitelisting**.
- Use **virtualized environments** to execute OS environments or specific programs.
- Categorize data based on organizational value, and implement **physical and logical separation of networks** and data for different organizational units.
- Require user interaction for end-user applications communicating with websites uncategorized by the network proxy or firewall.

# Business Email Compromise

- **Business email compromise (BEC)** — also known as email account compromise (EAC)—is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business—both personal and professional.
- These sophisticated scams are carried out by fraudsters compromising email accounts and other forms of communication such as phone numbers and virtual meeting applications, through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.
- In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request, for example:
  - A vendor your company regularly deals with sends an invoice with an updated mailing address.
  - A company CEO asks her assistant to purchase dozens of gift cards to send out as employee rewards. She asks for the serial numbers so she can email them out right away.
  - A homebuyer receives a message from his title company with instructions on how to wire his down payment.





# BEC: Preventative Measures

- Use **secondary channels** or **two-factor authentication** to verify requests for changes in account information.
- Ensure the **URL** in emails is associated with the business/individual it claims to be from.
- Be alert to **hyperlinks** that may contain misspellings of the actual domain name.
- **Refrain from supplying login credentials or PII of any sort via email.** Be aware that many emails requesting your personal information may appear to be legitimate.
- **Verify the email address** used to send emails, especially when using a mobile or handheld device, ensure the sender's address appears to match who it is coming from.
- Ensure the settings in employees' computers are enabled to **allow full email extensions to be viewed.**
- **Monitor your personal financial accounts on a regular basis for irregularities,** such as missing deposits.

# Investment Scams

- Deceptive practice that induces investors to make purchases based on false information. These scams usually offer those targeted large returns with minimal risk. (Retirement, 401K, Ponzi, Pyramid, etc.).
- In 2023, the losses reported due to Investment scams became **the most of any crime type tracked by the IC3**.
  - Investment fraud losses rose from \$3.31 billion in 2022 to \$4.57 billion in 2023, a 38% increase.
- Within these numbers, **investment fraud with a reference to cryptocurrency** rose from \$2.57 billion in 2022 to \$3.96 billion in 2023, an increase of 53%.
  - These scams are designed to entice those targeted with the promise of lucrative returns on their investments.
  - These scams can start with a simple text message from an unknown source.



# Tech Support & Government Impersonation Scams

- Subject posing as technical or customer support/service.
- Impersonation scams defraud thousands of individuals each year. Two categories of fraud reported to IC3, Tech/Customer Support and Government Impersonation, are responsible for over \$1.3 billion in losses.
- Call centers overwhelmingly target older adults, with devastating effects. Almost half the complainants report to be Over 60 (40%), and experience 58% of the losses (over \$770 million).
- **FBI Knoxville Cyber Squad:** The initial complaint received from IC3 spearheaded the investigation by identifying the main subjects, Ankur Khemani, and the Sterks, a family based in Iowa.
  - Khemani and his co-conspirators duped thousands of victims into believing their computers were infected with malicious malware.
  - Investigation grew from 50 initial IC3 reports to over 14,000 victims with over \$4 million in losses.
  - In 2023, Khemani was sentenced to 75 months for orchestrating a fraudulent computer technical support ring based in India.
  - In 2023, three members of the Sterk family were sentenced in Knoxville federal court for their involvement in a tech support scheme.





# Business Considerations to Address Cyber Threats



- **A culture of Information Security – Tone at the top**
- **A Structured Incident Response Plan**
- **Identify, Communicating and Protecting the Companies Crown Jewels**
- **Partnering with LE **before** an incident is crucial**
- **All executives should be involved in understanding risks/vulnerabilities.**
- **Communication is key**

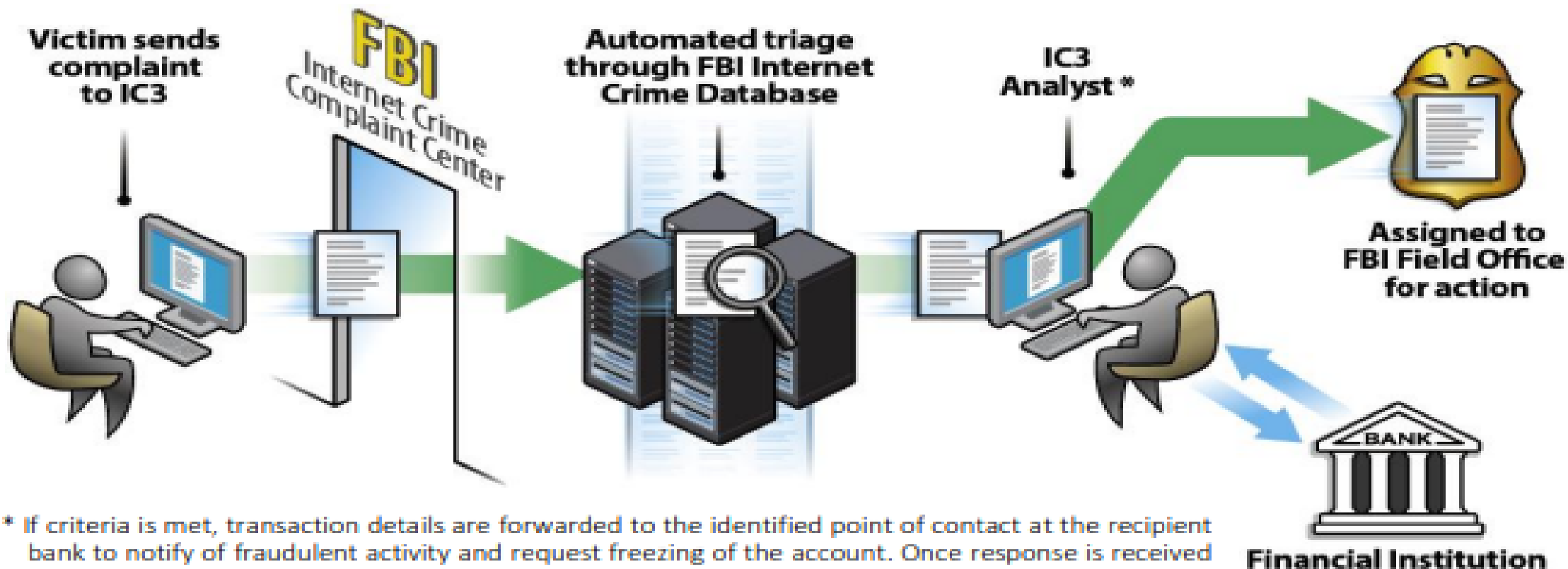
# Benefits of Working with FBI *Before* An Incident

- Increased optics into nefarious cyber activity enhances law enforcement operations - may increase capability of addressing a risk **before** it becomes a threat or actual incident.
- Opportunity to discuss response posture possibly reducing costs of responding to cyber attack.
- Basic understanding of requirements of private industry and U.S. government allowing for better prioritization of resources.
- Victim-modeling – FBI must take into consideration needs of an organization when determining if/when/how to share information.
- Whole-of-nation approach to combatting cyber threats.

# IC3 Recovery Asset Team

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 victims who made transfers to domestic accounts under fraudulent pretenses.

## RAT Process<sup>5</sup>



\* If criteria is met, transaction details are forwarded to the identified point of contact at the recipient bank to notify of fraudulent activity and request freezing of the account. Once response is received from the recipient bank, RAT contacts the appropriate FBI field office(s).

# Recovery Asset Team Success

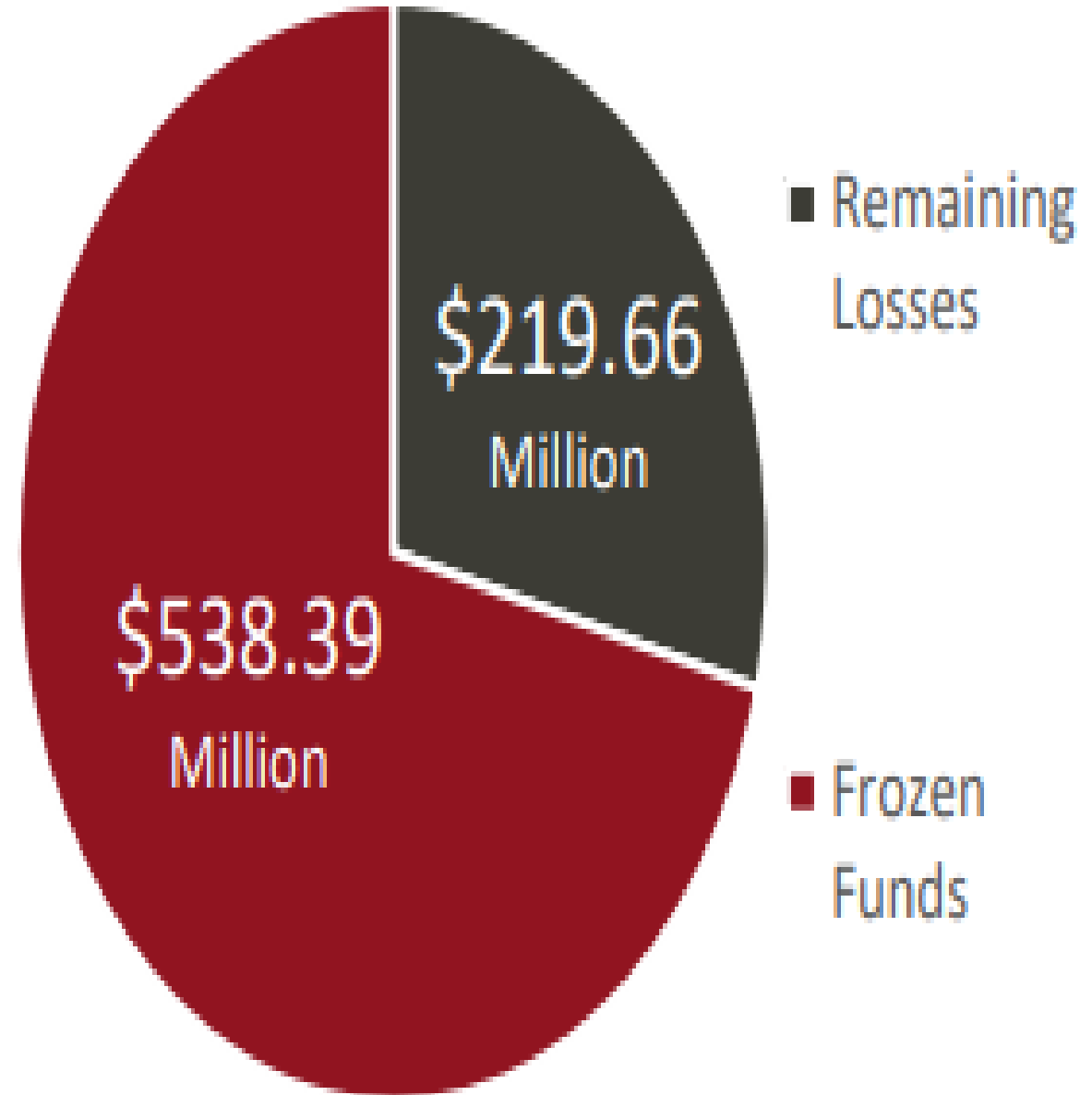
**Success to Date**

**71%** Success Rate

**3,008** Incidents

**\$758.05 Million** Losses

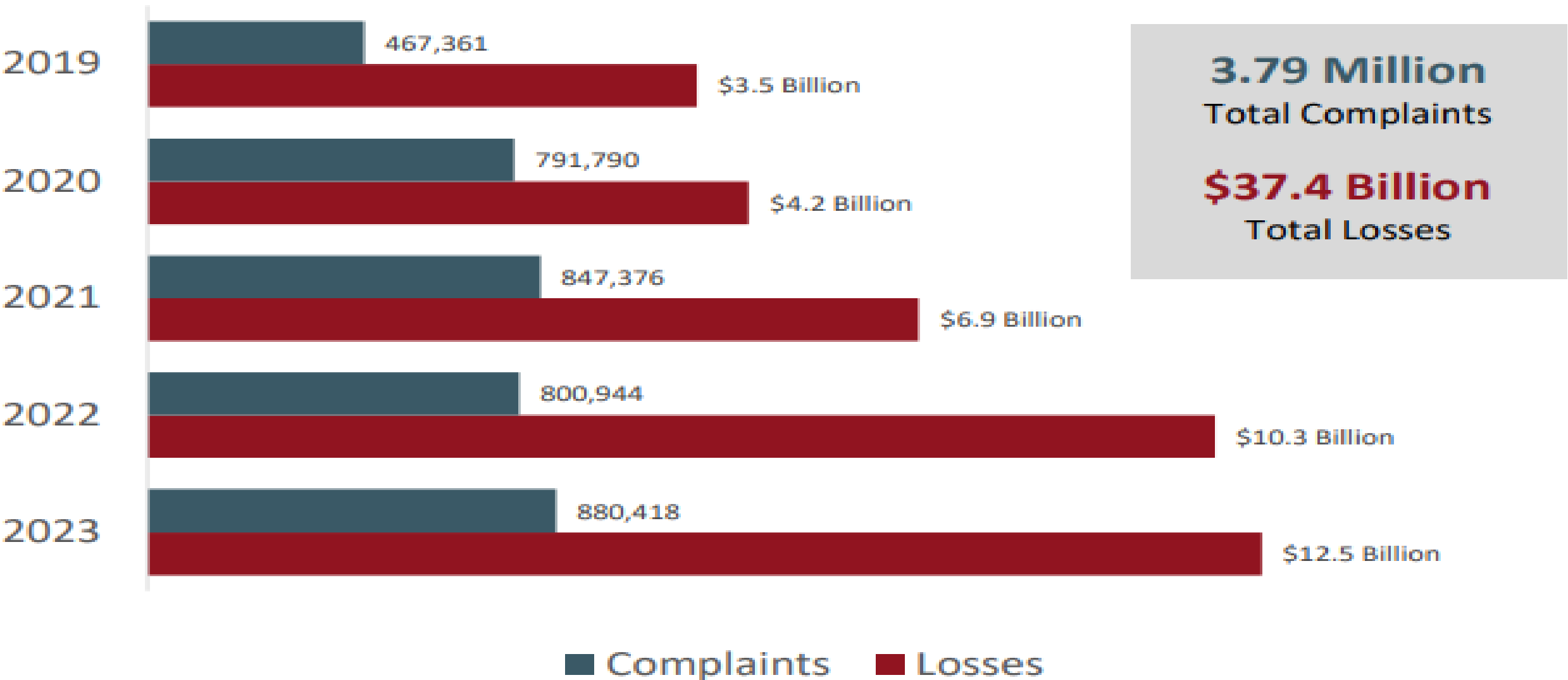
**\$538.39 Million** Frozen





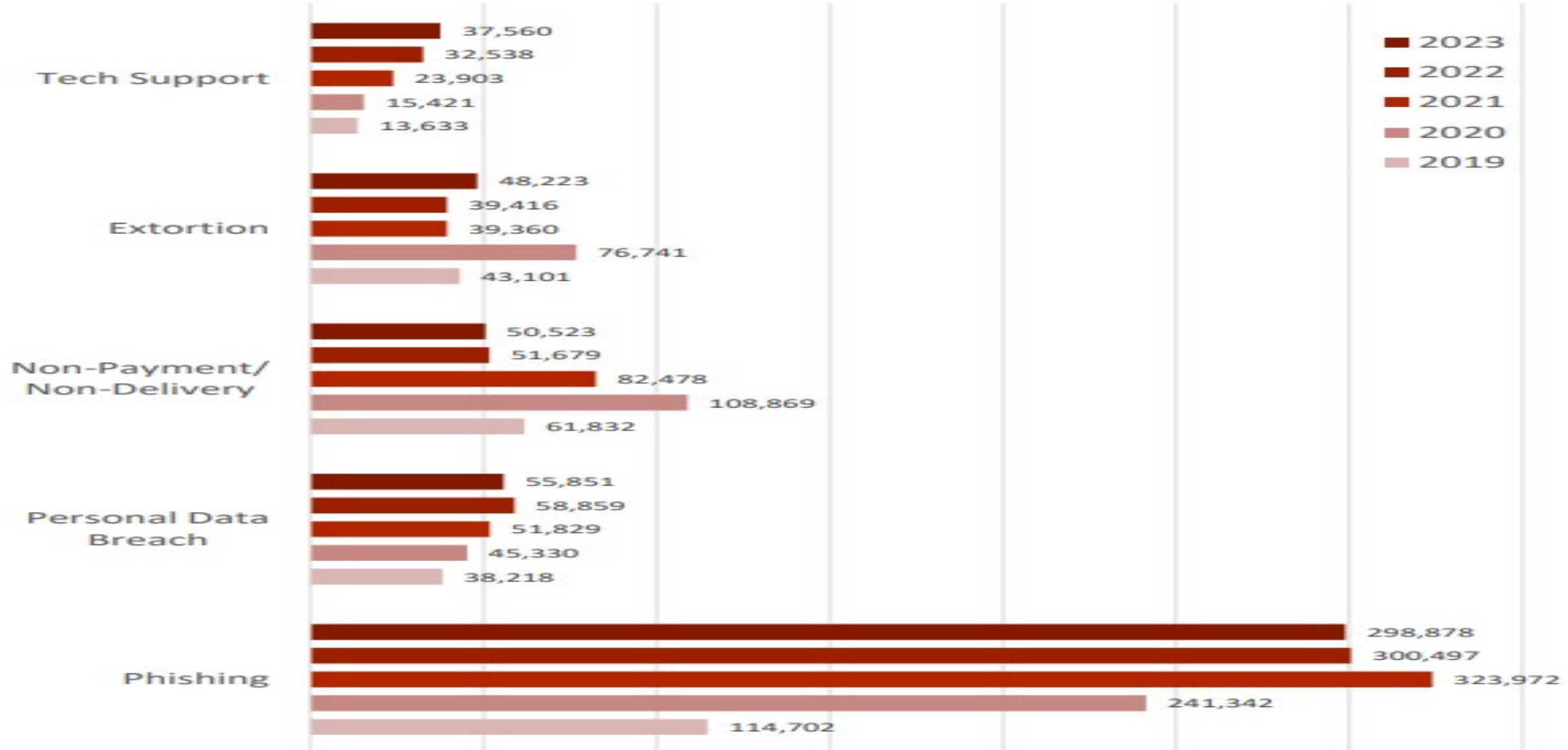
# IC3 Complaints Statistics

## Complaints and Losses over the Last Five Years\*



# Top Five Crime Types

## Top Five Crime Types Compared with the Previous Five Years



# 2023 Crime Types by Complaint Loss

## By Complaint Loss

<i>Crime Type</i>	<i>Loss</i>	<i>Crime Type</i>	<i>Loss</i>
<b>Investment</b>	\$4,570,275,683	<b>Extortion</b>	\$74,821,835
<b>BEC</b>	\$2,946,830,270	<b>Employment</b>	\$70,234,079
<b>Tech Support</b>	\$924,512,658	<b>Ransomware*</b>	\$59,641,384
<b>Personal Data Breach</b>	\$744,219,879	<b>SIM Swap</b>	\$48,798,103
<b>Confidence/Romance</b>	\$652,544,805	<b>Overpayment</b>	\$27,955,195
<b>Data Breach</b>	\$534,397,222	<b>Botnet</b>	\$22,422,708
<b>Government Impersonation</b>	\$394,050,518	<b>Phishing/Spoofing</b>	\$18,728,550
<b>Non-payment/Non-Delivery</b>	\$309,648,416	<b>Threats of Violence</b>	\$13,531,178
<b>Other</b>	\$240,053,059	<b>Harassment/Stalking</b>	\$9,677,332
<b>Credit Card/Check Fraud</b>	\$173,627,614	<b>IPR/Copyright and Counterfeit</b>	\$7,555,329
<b>Real Estate</b>	\$145,243,348	<b>Crimes Against Children</b>	\$2,031,485
<b>Advanced Fee</b>	\$134,516,577	<b>Malware</b>	\$1,213,317
<b>Identity Theft</b>	\$126,203,809		
<b>Lottery/Sweepstakes/Inheritance</b>	\$94,502,836		

# 2023 Crime Types by Complaint Loss

By Complaint Loss		▼ ▲ = Trend from previous Year			
Crime Type	2023		2022		2021
Advanced Fee	\$134,516,577	▲	\$104,325,444	▲	\$98,694,137
BEC	\$2,946,830,270	▲	\$2,742,354,049	▲	\$2,395,953,296
Botnet	\$22,422,708	▲	\$17,099,378	▲	N/A
Confidence Fraud/Romance	\$652,544,805	▼	\$735,882,192	▼	\$956,039,739
Credit Card/Check Fraud	\$173,627,614	▼	264,148,905	▲	\$172,998,385
Crimes Against Children	\$2,031,485	▲	\$577,464	▲	\$198,950
Data Breach	\$534,397,222	▲	\$459,321,859	▲	\$151,568,225
Employment	\$70,234,079	▲	\$52,204,269	▲	\$47,231,023
Extortion	\$74,821,835	▲	\$54,335,128	▼	\$60,577,741
Government Impersonation	\$394,050,518	▲	\$240,553,091	▲	\$142,643,253
Harassment/Stalking	\$9,677,332	▲	\$5,621,402		N/A
Identity Theft	\$126,203,809	▼	189,205,793	▼	\$278,267,918
Investment	\$4,570,275,683	▲	\$3,311,742,206	▲	\$1,455,943,193
IPR/Copyright and Counterfeit	\$7,555,329	▲	\$4,591,177	▼	\$16,365,011
Lottery/Sweepstakes/Inheritance	\$94,502,836	▲	\$83,602,376	▲	\$71,289,089
Malware	\$1,213,317	▼	\$9,326,482	▲	\$5,596,889
Non-Payment/Non-Delivery	\$309,648,416	▲	\$281,770,073	▼	\$337,493,071
Other	\$240,053,059	▲	\$117,686,789	▲	\$75,837,524
Overpayment	\$27,955,195	▼	\$38,335,772	▲	\$33,407,671
Personal Data Breach	\$744,219,879	▲	\$742,438,136	▲	\$517,021,289
Phishing/Spoofing	\$18,728,550	▼	\$160,015,411	▲	\$126,383,513
Ransomware	\$59,641,384	▲	\$34,353,237	▼	\$49,207,908
Real Estate	\$145,243,348	▼	\$396,932,821	▲	\$350,328,166
SIM Swap	\$48,798,103	▼	\$72,652,571		N/A
Tech Support	\$924,512,658	▲	\$806,551,993	▲	\$347,657,432
Threats of Violence	\$13,531,178	▲	\$4,972,099		N/A

# Crime Types by Complaint Count

By Complaint Count						
<i>Crime Type</i>	<i>2023</i>		<i>2022</i>		<i>2021</i>	
		▼ ▲ =				Trend from previous Year
<b>Advanced Fee</b>	<b>8,045</b>	▼	11,264	▲	11,034	▼
<b>BEC</b>	<b>21,489</b>	▼	21,832	▲	19,954	▲
<b>Botnet</b>	<b>540</b>	▼	568		N/A	
<b>Confidence Fraud/Romance</b>	<b>17,823</b>	▼	19,021	▼	24,299	▲
<b>Credit Card/Check Fraud</b>	<b>13,718</b>	▼	22,985	▲	16,750	▼
<b>Crimes Against Children</b>	<b>2,361</b>	▼	2,587	▲	2,167	▼
<b>Data Breach</b>	<b>3,727</b>	▲	2,795	▲	1,287	▼
<b>Employment</b>	<b>15,443</b>	▲	14,946	▼	15,253	▼
<b>Extortion</b>	<b>48,223</b>	▲	39,416	▲	39,360	▼
<b>Government Impersonation</b>	<b>14,190</b>	▲	11,554	▲	11,335	▼
<b>Harassment/Stalking</b>	<b>9,587</b>	▼	11,779		N/A	
<b>Identity Theft</b>	<b>19,778</b>	▼	27,922	▼	51,629	▲
<b>Investment</b>	<b>39,570</b>	▲	30,529	▲	20,561	▲
<b>IPR/Copyright and Counterfeit</b>	<b>1,498</b>	▼	2,183	▼	4,270	▲
<b>Lottery/Sweepstakes/Inheritance</b>	<b>4,168</b>	▼	5,650	▼	5,991	▼
<b>Malware</b>	<b>659</b>	▼	762	▼	810	▼
<b>Non-Payment/Non-Delivery</b>	<b>50,523</b>	▼	51,679	▼	82,478	▼
<b>Other</b>	<b>8,808</b>	▼	9,966	▼	12,346	▲
<b>Overpayment</b>	<b>4,144</b>	▼	6,183	▲	6,108	▼
<b>Personal Data Breach</b>	<b>55,851</b>	▼	58,859	▲	51,829	▲
<b>Phishing/Spoofing</b>	<b>298,878</b>	▼	321,136	▼	342,494	▲
<b>Ransomware</b>	<b>2,825</b>	▲	2,385	▼	3,729	▲
<b>Real Estate</b>	<b>9,521</b>	▼	11,727	▲	11,578	▼
<b>SIM Swap</b>	<b>1,075</b>	▼	2,026		N/A	
<b>Tech Support</b>	<b>37,560</b>	▲	32,538	▲	23,903	▲
<b>Threats of Violence</b>	<b>1,697</b>	▼	2,224		N/A	

# Crime Types by Complaint Count

By Complaint Count						
<i>Crime Type</i>	<i>2023</i>	<i>▼ ▲ = Trend from previous Year</i>	<i>2022</i>	<i>2021</i>		
Advanced Fee	8,045	▼	11,264	▲	11,034	▼
BEC	21,489	▼	21,832	▲	19,954	▲
Botnet	540	▼	568		N/A	
Confidence Fraud/Romance	17,823	▼	19,021	▼	24,299	▲
Credit Card/Check Fraud	13,718	▼	22,985	▲	16,750	▼
Crimes Against Children	2,361	▼	2,587	▲	2,167	▼
Data Breach	3,727	▲	2,795	▲	1,287	▼
Employment	15,443	▲	14,946	▼	15,253	▼
Extortion	48,223	▲	39,416	▲	39,360	▼
Government Impersonation	14,190	▲	11,554	▲	11,335	▼
Harassment/Stalking	9,587	▼	11,779		N/A	
Identity Theft	19,778	▼	27,922	▼	51,629	▲
Investment	39,570	▲	30,529	▲	20,561	▲
IPR/Copyright and Counterfeit	1,498	▼	2,183	▼	4,270	▲
Lottery/Sweepstakes/Inheritance	4,168	▼	5,650	▼	5,991	▼
Malware	659	▼	762	▼	810	▼
Non-Payment/Non-Delivery	50,523	▼	51,679	▼	82,478	▼
Other	8,808	▼	9,966	▼	12,346	▲
Overpayment	4,144	▼	6,183	▲	6,108	▼
Personal Data Breach	55,851	▼	58,859	▲	51,829	▲
Phishing/Spoofing	298,878	▼	321,136	▼	342,494	▲
Ransomware	2,825	▲	2,385	▼	3,729	▲
Real Estate	9,521	▼	11,727	▲	11,578	▼
SIM Swap	1,075	▼	2,026		N/A	
Tech Support	37,560	▲	32,538	▲	23,903	▲
Threats of Violence	1,697	▼	2,224		N/A	



# Threat Informed Defense

## *Special Presentation for the NAIC*

**Gregory Crabb**

*July 9, 2024*



# What is Threat Informed Defense

A cybersecurity approach that integrates threat intelligence into security strategy, focusing on understanding and countering an adversaries' tactics, techniques, and procedures.

---

## Six Steps Mastery

**Identify:** Understand the threats.

**Define:** Define intelligence needs.

**Prioritize:** Prioritize assets and services.

**Collect and Analyze:** Collect and analyze information.

**Decide and Communicate:** Make informed decisions and communicate effectively.

**Improve:** Continuously improve your threat intelligence program.

## Benefits:

Ready

Responsive

Resilient



# Chinese Government Poses 'Broad and Unrelenting' Threat to U.S. Critical Infrastructure



“And what many Americans may not be tracking closely is that China is positioning its enormous hacking enterprise—remember, 50 to 1—....to give itself the ability to physically wreak havoc on our critical infrastructure at a time of its choosing.”

“Companies need to familiarize themselves with each specific threat and its particularities, create a plan tailored to each of those threats, and then actually run through those plans with tabletop exercises. Most importantly, know where your crown jewels are, know how to get back up and running in the event of a breach, and know at what point you’re going to call the FBI for help.”

- FBI Director Christopher Wray, April 18, 2024

# Step 1: Identify ([FBI IC3 Alerts](#))

<b>Year:</b>	<b>Number of Alerts:</b>	<b>Types of Attacks:</b>
<b>2024</b>	<b>27 (So far)</b>	Social Engineering, <i>Ransomware</i> , Phishing, Secure by Design, State-Sponsored, AI Threats, Living Off the Land, IoT/OT, Election Security, Misinformation Campaigns, Remote Access Trojan
<b>2023</b>	<b>43</b>	<i>Ransomware</i> , State-Sponsored, Data Extortion, Spearphishing, Firmware Memory Attacks, AI Security, <i>Supply Chain</i> , CVEs Exploits, Nation-State, Bot Networks, Social Engineering, Remote Access Software
<b>2022</b>	<b>40</b>	Business Email Compromise, Ransomware, State-Sponsored, Hacktivist DDoS, Credential Stuffing, Fraudulent Cryptocurrency, Data Extortion, Medical Device Vulnerabilities
<b>2021</b>	<b>35</b>	Log4Shell, APT Exploits, Ransomware, State-Sponsored, Financial Events, Water System Threats, Supply-Chain, Business Email Compromise, Synthetic Content, DDoS, IoT

# Cyber Risk:

## Step 2: Define

Risk = Likelihood x Impact, where  
Likelihood =  $f(\text{Threat, Vulnerability})$

### Threat:

- The intent and capability to cause harm. The components of a threat include the **actors**, their **motives**, and their **capabilities**.

### Vulnerability:

- An exposure or weakness an actor could leverage to cause harm to an organization.

### Control:

- A mechanism an organization can apply to reduce the likelihood or impact of a risk.

### Priority Intelligence Requirements:

- Key information your organization needs about threats to make informed decisions.

# Step 3: Prioritize

**“To understand the threat **you need to focus on the information most relevant to the situation.**”**

*Andrew McCabe 10-8, LLC*

- What are the assets and functions that are essential to your organizational context?
- What are the technology assets that deliver these — hardware, data, source code, cloud providers?



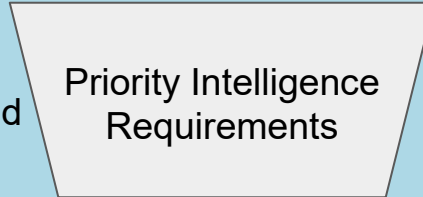
# Step 4: Collect and Analyze

Example:  
Cloud Attacks

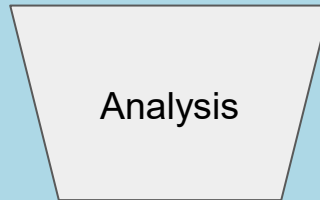


- CISA Known Exploited Vulnerabilities
- Organization specific systems
- Open Source Reporting
- Multi-State ISAC
- FBI Alerts
- And other sources

Example: How do regulated insurance companies assess and manage cloud vendor risk?








- Risk Assessment
- Gap Analysis
- Threat Modeling
- Scenario Planning
- Strategic Decisions
- Policy Updates



**Clear and actionable picture**

# Step 5: Decide and Communicate

	<b>Before and After Scenario Planning</b>	<p>Illustrate decision-making with a "before and after" scenario:</p> <ul style="list-style-type: none"><li>• <b>Before:</b> Potential chaos without acting (e.g., downtime, higher costs).</li><li>• <b>After:</b> Outcome with effective decisions (e.g., quick containment, reduce losses).</li></ul>
	<b>Decision Flow</b>	<p>Flowchart outlining the decision-making process once a threat is identified:</p> <ul style="list-style-type: none"><li>• <b>Decision points</b> (e.g., risk thresholds that trigger actions).</li><li>• <b>Possible actions</b> (e.g., increase monitoring, apply patches, escalate).</li><li>• <b>End results</b> (e.g., threat mitigated, ongoing monitoring, further investigation).</li></ul>
	<b>Case Study Timeline</b>	<p>Timeline of a real or hypothetical security incident, marking decision points:</p> <ul style="list-style-type: none"><li>• Initial identification or detection.</li><li>• Decision to escalate.</li><li>• Actions taken.</li><li>• Resolution and review.</li></ul>
	<b>Key Performance Indicators</b>	<p>Dashboard of KPIs measuring decisions and communications:</p> <ul style="list-style-type: none"><li>• <b>Time to decision.</b></li><li>• <b>Communication reach</b> (how many relevant parties were informed).</li><li>• <b>Outcome effectiveness</b> (measure of threat mitigation success).</li></ul>
	<b>Communication Matrix</b>	<p>Matrix showing who needs to be informed at various stages of the process:</p> <ul style="list-style-type: none"><li>• <b>Horizontal communication</b> (e.g., between departments or teams).</li><li>• <b>Vertical communication</b> (up to executives or down to operational teams).</li><li>• <b>External communication</b> (to vendors, partners, regulated entities or regulators).</li></ul>

# Step 6: Improve

**Identify:** Have you clearly defined what 'threat intelligence' means for your organizational context?

**Define:** Do you have well defined priority intelligence requirements and are they operationalized?

**Prioritize:** How effective are you at assessing new intelligence based on the prioritized assets and functions in your organizational context?

**Collect:** Do you have systematic processes for collecting data from multiple sources? And are you able to draw actionable insights from your threat intelligence?

**Communicate:** Do you have protocols in place for swift decision-making and communication based on intelligence?

**Improve:** Are you looking to improve your use of intelligence - skills and abilities, processes and technology?

Let's **make progress together** by collaborating in **the upcoming cohort of our free\* Six Steps to Mastery course**.

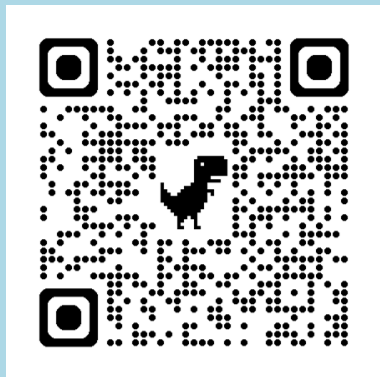
*\*Free for state government representatives.*

# Join the Six Steps to Mastery

Join us in the '10-8 Cyber Arena' to dive deep. To prepare for the threats we face, sign-up today to discuss, apply and action these steps for your organizational context.

Enroll at:

<https://www.teneightcyber.com/>



Rewatch This Presentation at:

<https://youtu.be/IZFfRuVgGrQ>

## **Six Steps to Mastery**

Navigate the complexities of threat intelligence with our guided journey through the six essential steps, empowering you to effectively anticipate and counteract cyber threats.

## **Intel Central**

Stay updated with the latest in cybersecurity through our daily and weekly briefings, and engage in member-led discussions to explore diverse perspectives and real-world incident analyses.

## **Live Cyber Hub**

Join our scheduled live events to discuss current cyber threats and strategies with experts and community members.

## **Ransomware Radar**

Study the evolving world of ransomware with detailed profiles on threat groups, victim organizations, and their latest tactics, techniques and procedures.