

Cybersecurity Collaboration: Cyber Threats to the Forest Products Industry & Federal Resources

2022 PPSA Conference



June 23, 2022

1

UNCLASSIFIED

Mission



Impose risk and consequences on cyber adversaries through unique authorities, world-class capabilities, and enduring partnerships, building upon a century of innovation.



Lead the national effort to **understand** and **manage** cyber and physical **risk** to our critical infrastructure.



June 23, 2022

UNCLASSIFIED

Roles and Responsibilities



CYBERSECURITY RESPONSIBILITIES



History and Organization



- Established in 2018
- Defend against today's threats and collaborates to build more secure and resilient infrastructure
- 10 Regions
- Operations, Intelligence, and Outreach

-
- Established in 2002
 - Investigates Computer Intrusions
 - Criminal and National Security
 - 56 Field Offices and International Presence
 - Operations, Intelligence, and Outreach



June 23, 2022

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient critical infrastructure for the American people.

MISSION

Lead the national effort to understand and manage cyber and physical risk to our critical infrastructure.

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Who We Are

CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.



FEDERAL NETWORK
PROTECTION



PROACTIVE CYBER
PROTECTION



INFRASTRUCTURE
RESILIENCE &
FIELD OPERATIONS



EMERGENCY
COMMUNICATIONS



CORE COMPETENCIES

Partnership Development

CISA fosters collaborative partnerships that enable partners in the government and private sector to make informed, voluntary decisions and investments.



Every day, CISA employees: Share information with critical infrastructure partners and stakeholder and serve as the national hub for cybersecurity and communications information data sharing in near-real-time.



Sector outreach: CISA works with government officials and critical infrastructure stakeholders to plan, develop and facilitate exercises that build capacity, improve security and bolster resilience.

Critical Infrastructure Significance

- Critical Infrastructure refers to the assets, systems, and networks, whether physical or cyber, so vital to the Nation that their incapacitation or destruction would have a debilitating effect on national security, the economy, public health or safety, and our way of life



16 Sectors & Sector Specific Agencies

 CHEMICAL	DHS (CISA)	 FINANCIAL	Treasury
 COMMERCIAL FACILITIES	DHS (CISA)	 FOOD & AGRICULTURE	USDA & HHS
 COMMUNICATIONS	DHS (CISA)	 GOVERNMENT FACILITIES	GSA & DHS (FPS)
 CRITICAL MANUFACTURING	DHS (CISA)	 HEALTHCARE & PUBLIC HEALTH	HHS
 DAMS	DHS (CISA)	 INFORMATION TECHNOLOGY	DHS (CISA)
 DEFENSE INDUSTRIAL BASE	DOD	 NUCLEAR REACTORS, MATERIALS AND WASTE	DHS (CISA)
 EMERGENCY SERVICES	DHS (CISA)	 TRANSPORTATIONS SYSTEMS	DOT & DHS
 ENERGY	DOE	 WATER	EPA



June 23, 2022

9

UNCLASSIFIED

Threats to Critical Infrastructure

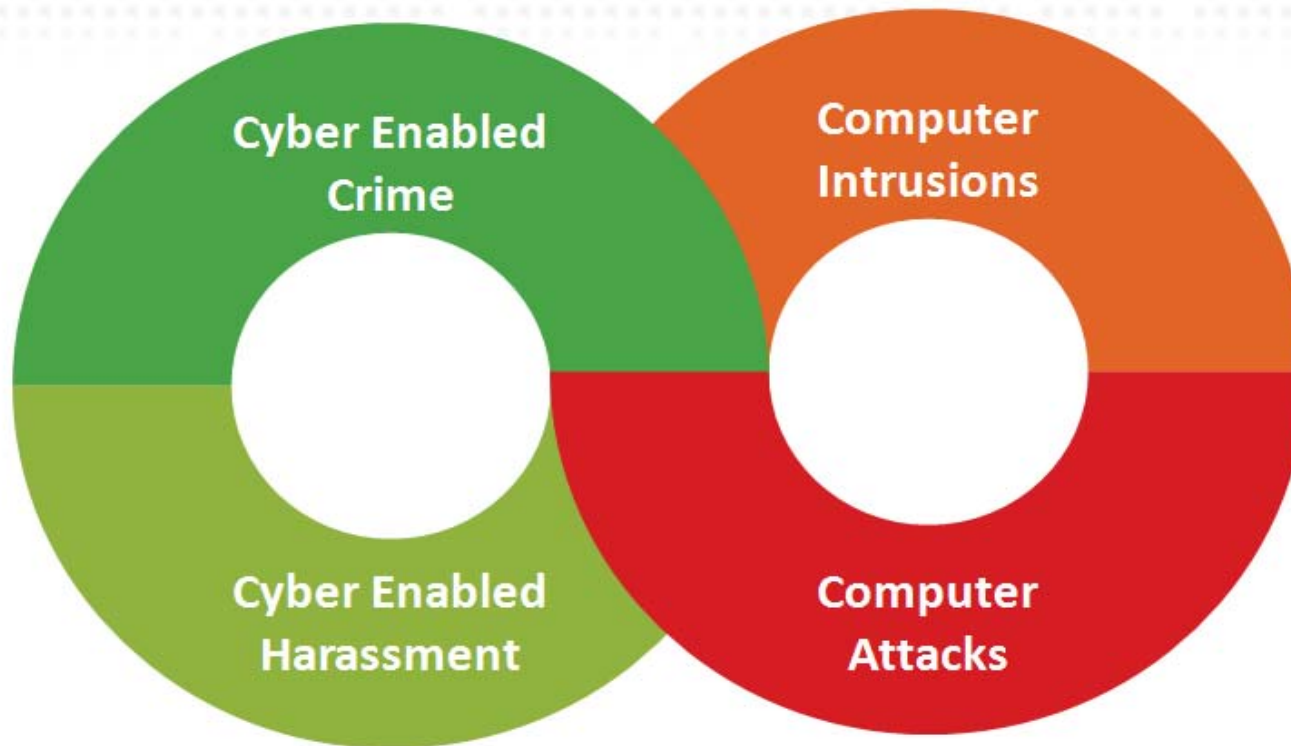
- Critical infrastructure remains at risk from a variety of threats including:

- Extreme Weather
- Pandemics
- Accidents / Technical Failures
- Acts of Terrorism
- Cyber Attacks
 - Ransomware





Types of Malicious Cyber Activity



UNCLASSIFIED//FOR OFFICIAL USE ONLY

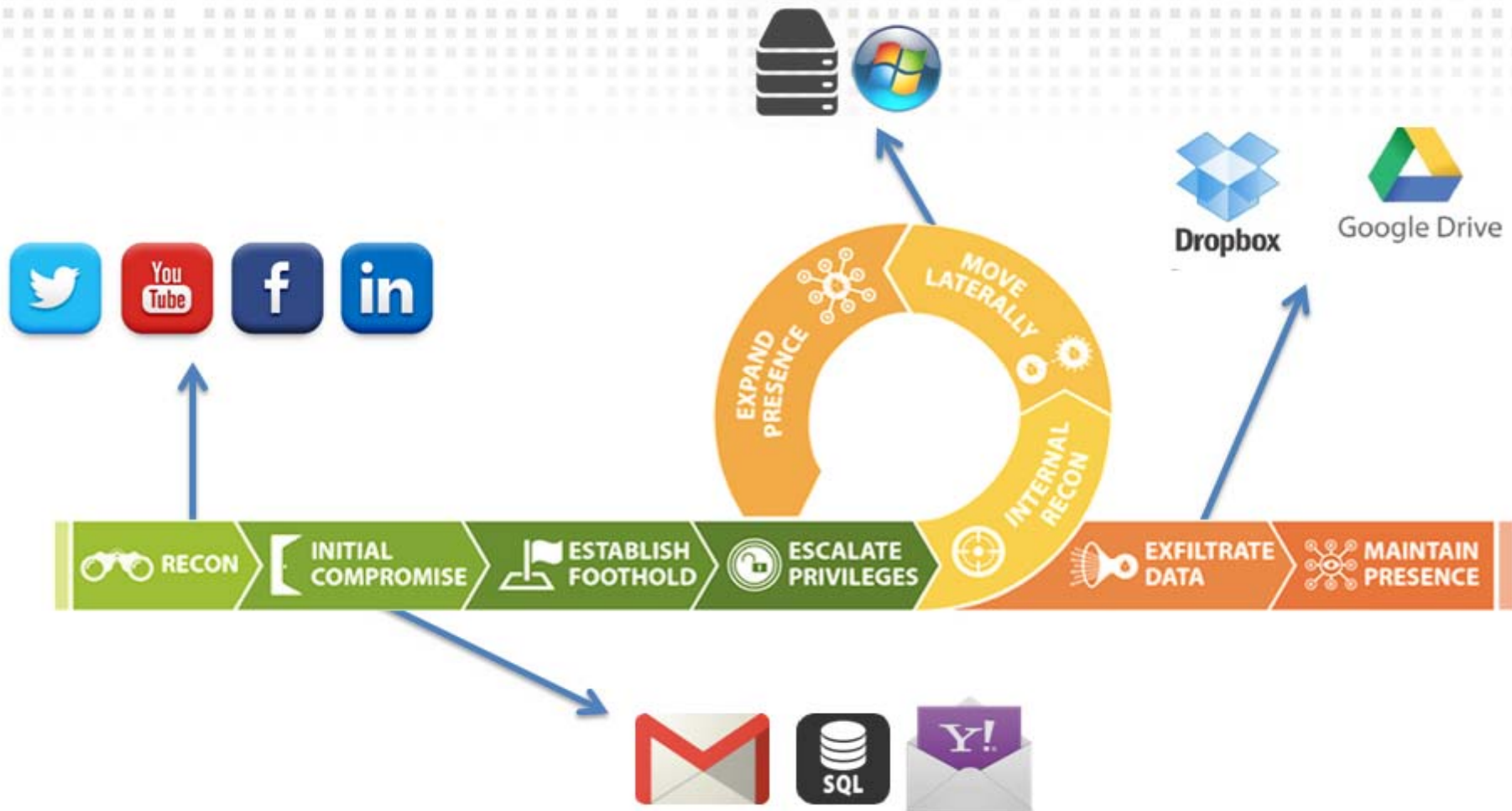


Cyber Threats





On The Network



Legitimate business services can be used for illicit cyber acts



Types of Attack



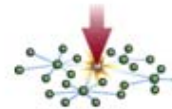
DDoS



False Tax Return Filings



Doxing



Network Destruction
Attacks



Theft of IP



Ransomware and
Extortion



Theft of PII, PHI



Business E-mail
Compromise



Point of Sale Breaches



Website Defacements



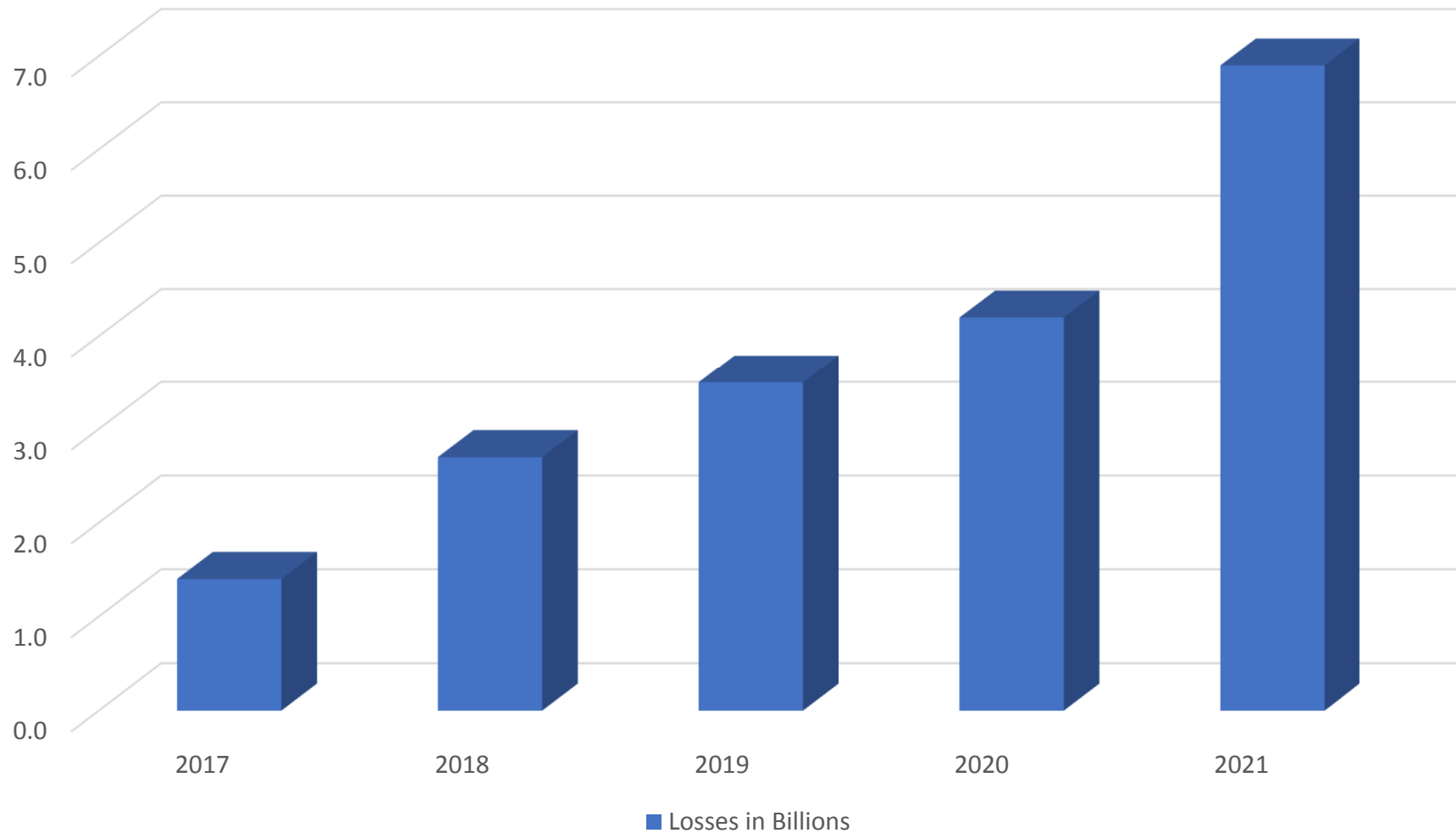
Internet Crime Complaint Center (IC3)



- Report Internet-facilitated criminal activity to the FBI (www.ic3.gov)
- Information analysis and dissemination to law enforcement
- Prevention tips and scheme descriptions
- Facilitate asset recovery



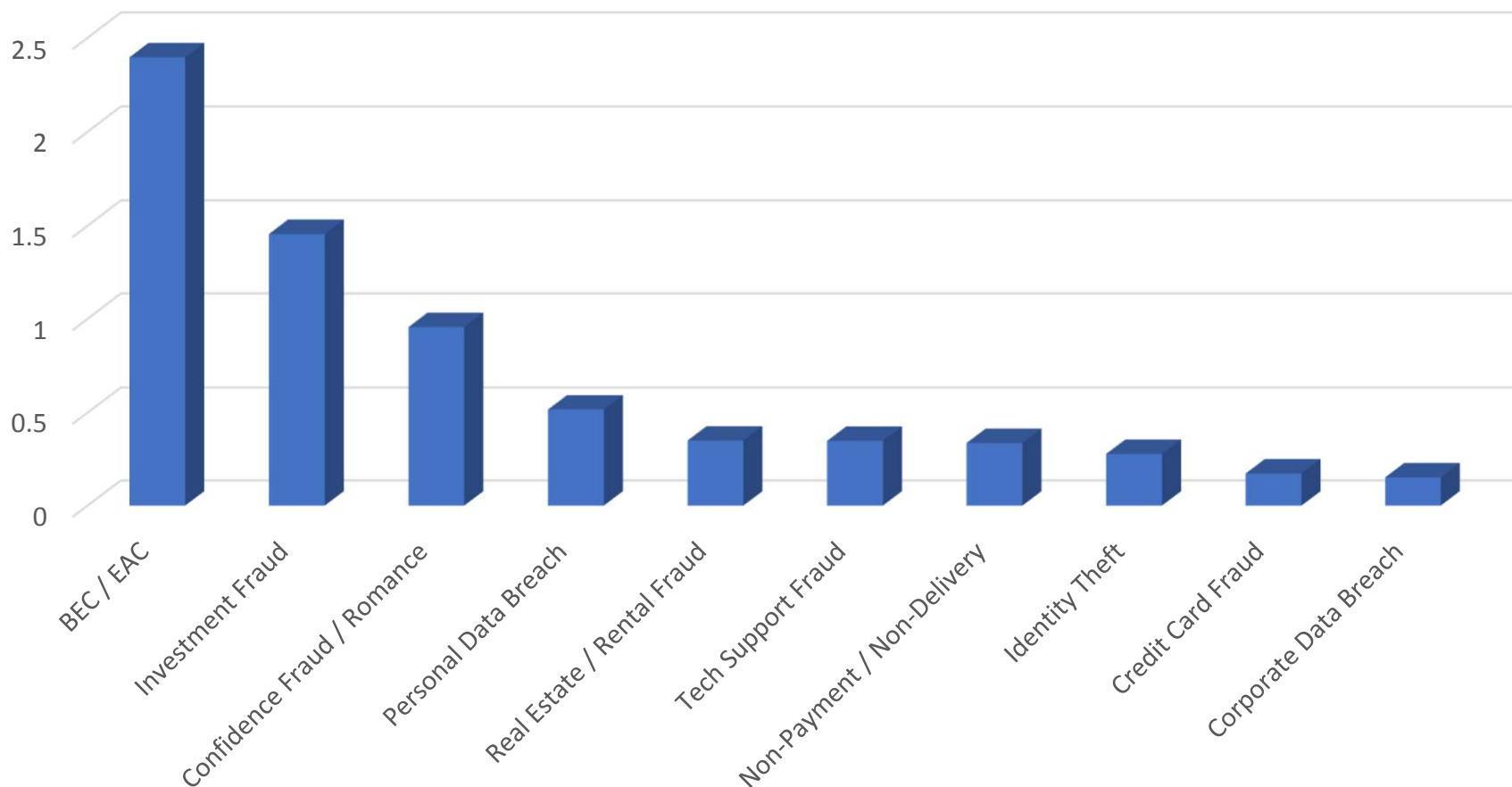
Sum Losses Reported to IC3





Top 10 Crimes Reported to IC3

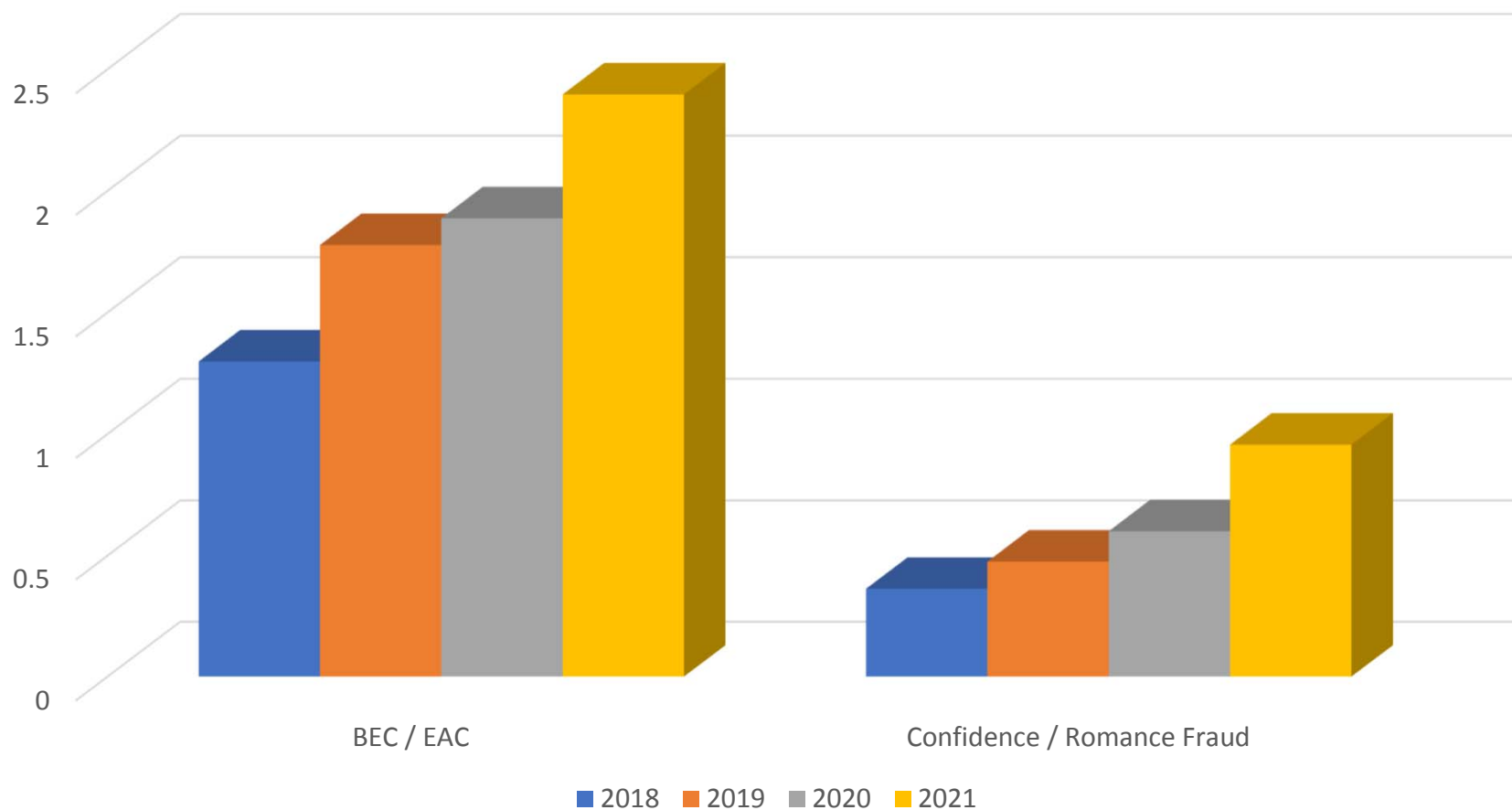
Losses in Billions (2021 Data)





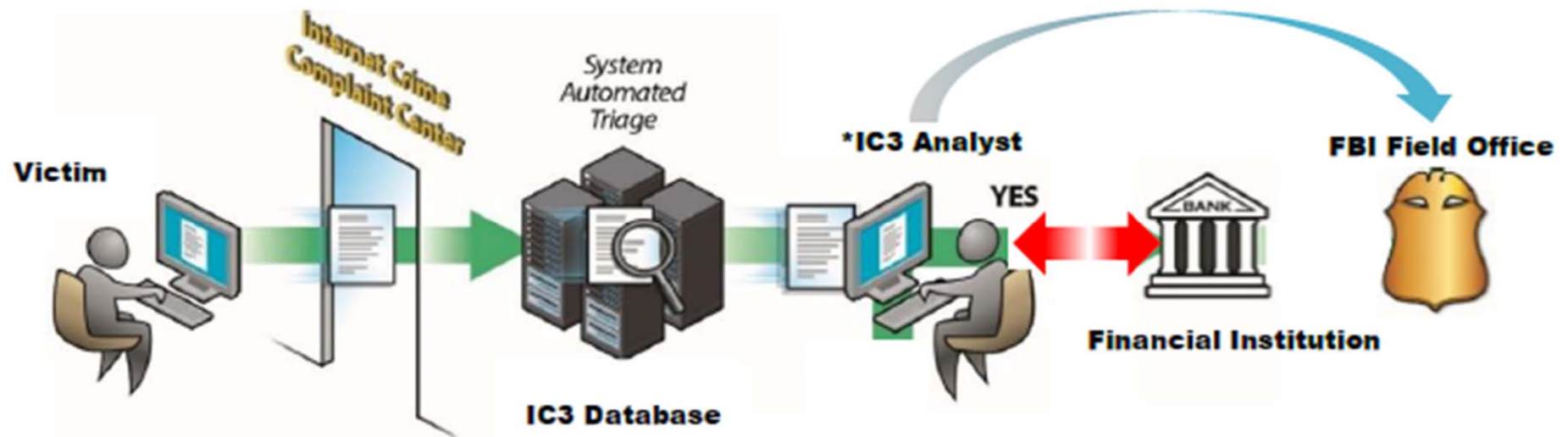
Growing Losses for BEC / Romance

Losses in Billions (2021 Data)





IC3 Recovery Asset Team (RAT)



Successes in 2020



Incidents: 1,303

Losses: \$463 Million

Frozen: \$380 Million

Cybersecurity Assessments

- **Cyber Resilience Review (Strategic)**
- **External Dependencies Management (Strategic)**
- **Cyber Infrastructure Survey (Strategic)**
- **Cybersecurity Evaluations Tool (Strategic)**
- **Phishing Campaign Assessment**
- **Validated Architecture Design Review (Technical)**
- **Vulnerability & Web App Scanning (Technical)**
- **Remote Penetration Test (Technical)**
- **Risk and Vulnerability Assessment (Technical)**



June 23, 2022

20

Additional Resources & Services

- Information sharing
 - Threat intelligence
 - Vulnerability information
- Hometown Security
 - Connect
 - Plan
 - Train
 - Report
- Vulnerability assessments
- Training, education, & exercises
 - Active shooter
 - Insider Threat
 - De-escalation
 - Counter improvised explosive devices
 - Protective measures





To enroll in CISA services, more information, or your local CISA contact:

CISA

PSA / TFO Kirby Wedekind

Cell: 202-868-1361

Email: Kirby.Wedekind@HQ.DHS.GOV

For more information:

cisa.gov/

cisa.gov/cybersecurity

ic3.gov

PSA Kirby Wedekind
June 23, 2022