Cyber Incident Reporting Framework

How to streamline and facilitate information sharing

By Megan Stifel and Zoë Brammer
The Institute for Security and Technology
AGENDA

- Ransomware problem statement
- Incident reporting state of play
- Practical guidance for national reporting regimes
- Existing frameworks for exchange of information
- Resources

Megan Stifel
Chief Strategy Officer, IST, Co-Chair, Ransomware Task Force

Zoë Brammer
Cyber & Information Operations Senior Analyst, IST
FinCEN Analysis Reveals Ransomware Reporting in BSA Filings Increased Significantly During the Second Half of 2021

Immediate Release: November 01, 2022

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) today issued its most recent Financial Trend Analysis of ransomware-related Bank Secrecy Act (BSA) filings for 2021, indicating that ransomware continued to pose a significant threat to U.S. critical infrastructure sectors, businesses, and the public. The report focuses on ransomware trends in BSA filings from July-December 2021, and addresses the extent to which a substantial number of ransomware attacks appear to be connected to actors in Russia.

“Today’s report reminds us that ransomware—including attacks perpetrated by Russian-linked actors—remain a serious threat to our national and economic security,” said FinCEN Acting Director Himamraul Das. “It also underscores the importance of BSA filings, which allow us to uncover trends and patterns in support of whole-of-government efforts to prevent and combat ransomware attacks. Financial institutions play a critical role in helping to protect the United States from ransomware-related threats simply by fulfilling their BSA compliance obligations.”
Best practices for reporting frameworks

● Outline the purpose of reporting
  ○ Trend identification
  ○ Indication and early warning
  ○ Incident response
  ○ Assessing impact and harm

● Provide clear guidelines for reporting and outline how information will be used

● Must build trust on confidentiality of reported information

● Minimize the burden on reporting entities by “one-stop-shop” for reporting.
Internationally, utilize existing mechanisms for sharing
Zoë: zoe@securityandtechnology.org

Megan: megan@securityandtechnology.org