Brian Sowers

11/10/2023

Threat Intelligence and Intelligence Sharing

1. Identify two specific cybersecurity threat intelligence sources you should monitor and explain why they are valuable to the industry as a whole.

Financial Intelligence (FININT) and Cyber Intelligence (CYBINT) are critical cybersecurity threat intelligence sources for the financial industry (Secure Business Operations Module 2, 9). FININT, delving into the financial motivations of attackers, provides essential insights for understanding economic incentives driving cyber threats. This understanding aids in targeted cybersecurity strategies and proactive risk management, ensuring the safeguarding of financial resources. On the other hand, CYBINT offers a holistic view of cyber threats by integrating disciplines like Signals Intelligence and Open-source Intelligence. This comprehensive approach enables financial institutions to detect, analyze, and respond to a diverse range of cybersecurity risks. For example, Citibank, is “using machine learning and big data to prevent criminal activities and monitor potential threats to customers in commerce” (Maskey, 1). The adaptability of CYBINT, incorporating different sources, ensures ongoing awareness of evolving cyber threats, empowering organizations to anticipate and counter emerging risks effectively. Monitoring both FININT and CYBINT sources equips the financial sector with nuanced intelligence, facilitating the implementation of tailored and robust cybersecurity measures.

2. Describe some of the regulatory or compliance standards for your sector that would impact the types of information you would share with your intelligence community in the future.

The regulatory landscape for the financial sector imposes stringent standards that significantly influence the nature of information shared within the intelligence community. Notably, the Financial Services Information Sharing and Analysis Center (FS-ISAC) adopted the STIX architecture (including CybOX) in Q2 2012, establishing a cyber threat information-sharing framework among its constituent members in the financial services sector. “Structured Threat Information eXpression (STIX) is a quickly evolving, collaborative community-driven effort to define and develop a language to represent structured threat information” (STIX Whitepaper, 2).The implementation of STIX facilitated the creation of an operational threat information repository by FS-ISAC, accessible to its extensive membership of approximately 4200 organizations as of May 2013 (STIX Whitepaper, 19). This integration underscores the sector's commitment to standardized and structured information sharing, aligning with regulatory expectations. Compliance with such frameworks ensures that intelligence shared within the financial community adheres to established standards, enhancing collective cybersecurity resilience.

Works Cited

Barnum, Sean. “Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression.” *MITRE*. https://panacademy.net/CourseFiles/sbo/Structured_Threat_Information.pdf. Accessed: 10 November 2023.

Maskey, Sameer. “How Artificial Intelligence Is Helping Financial Institutions.” *Forbes.* https://www.forbes.com/sites/forbestechcouncil/2018/12/05/how-artificial-intelligence-is-helping-financial-institutions/?sh=2f344c0460a4. Accessed: 10 November 2023.

“Secure Business Operations Module 2”, https://s3.amazonaws.com/assets.paloaltonetworksacademy.net/sbo/Business_Operations_Module_1.pdf. Accessed: 10 November 2023.