Threat Intelligence Programs
Questions Board Members Should Ask

Below are some questions you may ask management to ensure that the institution has a threat intelligence program that allows the institution to gather, analyze, and act upon threat information before negative impacts occur.

1. ***How does the institution gather, analyze, and act on threat intelligence?***

   WHY THIS IS IMPORTANT: There are a variety of threat intelligence resources that financial institutions can leverage to gather this information. The most common sources include, but are not limited to:

   - *FS-ISAC and MS-ISAC: Information-sharing communities that deliver real-time alerts and sector-specific intelligence. U.S. institutions with less than $1B in assets can maintain a cost-free membership with FS-ISAC's Critical Notification Only Participant (CNOP) program.*
   - *FBI InfraGard: Connects financial institutions with law enforcement for information sharing and early warnings*
   - *CISA Programs and Alerts: Offers updates on vulnerabilities, malware campaigns, and best practices from the U.S. government*
   - *Open Threat Exchange (OTX) and other community-driven threat exchange platforms*
   - *Subscriptions to newsfeeds from industry cybersecurity websites*
   - *Communications and alerts sent directly from applicable hardware and software vendors*
   - *Vendor-sponsored CISO user groups*

   It is important to have a process to disseminate threat information to appropriate IT/Security personnel in a timely manner.

2. ***Does the institution's threat intelligence program incorporate a process for managing and acting upon threat information?***

   WHY THIS IS IMPORTANT: Having a ***mechanism to manage the myriad available threat information*** *is essential to navigate through the noise of irrelevant or untimely information. To really make the most sense of threats that might impact the institution, it is important to remember a couple of key requirements. First, it is extremely beneficial to* ***understand the institution's own operating environment****, as well as* ***interactions that assets have with one another within the institution's operating environment****. The point is that there is not always a singular effect on a specific asset when threats materialize. Understanding not only the threats that exist, but also how these threats, if materialized, might impact overall operations is a good means of* ***triaging threat information and prioritizing responses and preparing recovery strategies for mission critical processes*** *within the institution. And because threats often require swift actions to address, it is important that IT security teams are well-equipped to* ***act upon threat intelligence information*** *once it's received, analyzed, and prioritized.*

3. ***Does the institution participate in an information-sharing organization to receive and share threat information?***

   WHY THIS IS IMPORTANT: According to NIST, "Most organizations already produce multiple types of cyber-threat information that are available to share internally as part of their IT and security operations efforts." ***When a financial institution participates in an information sharing mechanism, others benefit from "the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face.*** *Using this knowledge, an organization can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies. By correlating and analyzing cyber-threat information from multiple sources, an organization can also enrich existing information and make it more actionable. Organizations that receive threat information and subsequently use this information to remediate a threat confer a degree of protection to other organizations by impeding the threat's ability to spread."*[1]

4. ***Are we conducting regular threat scenario planning based on the top threats to our institution?***

   WHY THIS IS IMPORTANT: The vast majority of IT assets used in financial institutions today are exposed to a constantly changing and perpetually dangerous threat environment. Threat modeling allows the institution to leverage intelligence to ***help identify specific threats to critical assets or processes*** *and* ***design and test specific countermeasures to lessen the risk from these threats****. In addition, this same threat intelligence can also help* ***to inform the institution's incident and recovery scenario planning processes****. The goal is to recognize cyber threat-borne risks before they materialize, and robust, dynamic threat intelligence programs can be a principal driver in the success of these efforts across the entirety of the organization.*

[1] National Institute of Standards and Technology. Johnson, Chris, Feldman, Larry, and Witte, Greg (Editors). "ITL Bulletin for May 2017: Cyber-Threat Intelligence and Information Sharing". May 2017.