tracesecurity
Compliance, simplified.

Whitepaper

What We Risk: Common Cybersecurity Shortcomings of Financial Organizations in 2019

William Raziano
Information Security Analyst

Overview

Financial organizations represent a critical sector of business, and the reduction of risk from threats to confidentiality, integrity, and availability (CIA) should be the highest-priority undertaking for these organizations. The intrinsic liquidity of financial organizations makes them desirable targets of unauthorized parties wishing to gain quick capital from a breach.

To combat these threats, many organizations execute risk assessments to determine the risks within various aspects of their institutional structure. Once a reliable set of risk metrics has been established, the organization begins the process of implementing controls to achieve multiple objectives, the most crucial objective being mitigating *residual risk*.

The National Institute of Standards and Technology (NIST) regularly publishes Cybersecurity Frameworks (CSF) that can be paired with the suggestions of various regulatory and advisory bodies, such as the Federal Financial Institutions Examination Council (FFIEC), to create successful cybersecurity programs. Once an organization has applied the industry-recommended standards, regular audits by a third party, such as TraceSecurity, publisher of this paper, verify what implementations are lacking, ongoing, or forthcoming.

TraceSecurity audited a sample set of 16 financial organizations utilizing secondary, non-descriptive data collection throughout the 2019 calendar year. These findings highlight the most common NIST CSF controls deemed “Not Implemented” at the end of the auditing process. While the scope of this whitepaper may not be quantitatively comprehensive, our analysis points to timely trends, broad tendencies, and typical cybersecurity shortcomings exhibited in the financial sector.

Findings & Analysis

The findings below are organized by asset group; controls are organized based on function:

- The Organization asset group contains the organization’s “administrative” controls, including governance through formalized procedures and policies, which are customarily reviewed and approved by the Board.
- The Personnel asset group contains the organization’s human resources controls, including the formalized policies and procedures in place to govern acceptable and expected employee activities, roles, and responsibilities.
- The Physical and Environmental asset group includes the implementation of controls to monitor and protect critical systems and sensitive areas.
- The Technical Assets group is a parent-level control group containing many sub-groups, including Network, Systems, and Applications.
- The Network asset group primarily concerns the physical and logical implementations and controls that are put into place to separate and protect the organization’s network from the Internet.

- The Records asset group contains controls designed to protect records, information, and data that is vital to the organization, or that holds sensitive data.
- The Systems asset group contains controls designed to protect and harden managed endpoints and servers within the organization.
- The Applications asset group contains software assets that protect against threats to CIA.

Organizational Assets

A crucial function in the Organization asset control group is communication. Communication assets can be enhanced through an organization's policies, community participation in co-ops and other member groups, and cybersecurity awareness training.

While most organizations are well-equipped to handle internal communications, the task of educating a wider audience (like customers) on the importance of their own cybersecurity is much more daunting. An organization can and should create policies for employees and customers that regulate what specific information individuals can share. Defining what is shareable and what is private enhances accountability.

Membership in a co-op or a collection of organizations can be a great way to both gather and disseminate practical information and data. Member groups commonly share information on detection and protection methods, mechanisms, and solutions. This type of information sharing can benefit organizations of all sizes, complexities, and cybersecurity program maturity levels.

Perhaps the most beneficial communication asset is cybersecurity awareness training. Educating personnel (employees) and members (customers) on the methods, mechanisms, and practices employed by bad actors effectively prevents monetary loss.

Potential losses realized from personnel/member breaches can be expensive and far-reaching, sometimes even resulting in significant reputation damage to the organization. Cybersecurity awareness training, whether conducted in-house or by a third party, creates a robust defense against the culture of ignorance that leads to losses.

Personnel Assets

The Personnel asset group drives accountability. Often, an organization maintains adequate controls but fails to enforce them in the real world. Our findings show that organizations seldom practice actual testing of employees to verify adherence to their accountability standards and responsibilities.

A commonly successful attack vector is social engineering, which the organization or a third party should test annually. As an auditor, I have traveled to several different locations to audit financial organizations' cybersecurity controls.

During the vast majority of my onsite visits, I have not been asked by personnel for government-issued identification. This flaw stems from a lack of Visitor Escort policies and procedures or the practice

thereof. Verification of identity can thwart most social engineering attempts, yet it is the most overlooked aspect of physical access procedures.

Organizations should also consider testing Clean Desk policies and procedures, as unauthorized physical access by a social engineer can lead to further unauthorized access. Clean Desks testing includes the attempt to gain access to all readily available physical copies of Personally Identifiable Information, open systems, unlocked filing cabinets, and sensitive areas.

Physical & Environmental Assets

Environmental monitoring, including the implementation of sensors for fire, temperature, moisture, vibrations, and power issues, are essential for all organizations, especially those that house Data Centers and server rooms onsite. While not all organizations have site locations within known flood areas, the omnipresence of running water inside most modern buildings necessitates the implementation of a means to detect moisture regardless of location.

Organizations housing an onsite data center or server closet should consider installing a waterless fire suppression system. Additionally, the sensitive areas within an organization's sites should be monitored continuously against potential unauthorized access. The implementation of a surveillance system, especially a regularly monitored system, can alert security personnel of unauthorized access after business hours.

Technical Assets

Controls within the overarching Technical Assets group deal with hardware and software systems, including those that envelop the full-system life cycle, the performance and capacity of information assets, and the management of supply chain risks. A fully developed System Development Life Cycle includes identification and documentation of the full process of acquiring, configuring, deploying, maintaining, and, eventually, decommissioning of systems, devices, and other information assets.

Implementation of a System Development Life Cycle will improve an organization's ability to produce consistency across systems and environments. The maintenance of systems should include a real-time view of the performance and capacity of managed endpoints, servers, and devices for troubleshooting, detection, and preventative maintenance activities.

A comprehensive Supply Chain Risk Management program can lower the risks involved with some acquisition and implementation activities. Finally, all software, firmware, and hardware should reach the organization through secure channels.

Network Assets

Due to the proliferation of hacking methodologies, mechanisms, and toolsets, most organizations have relatively robust controls to maintain the perimeter of their network, which can keep most Internet-based attackers out under typical situations. However, attacks can occur from within the business network as well.

A social engineer can infiltrate through an unsecured wireless vector, by plugging a device into a hot network switch/port, or by engaging with an employee. Additionally, internal rogue elements could gain a foothold on the business network to exfiltrate sensitive information and data.

The methods used to protect the internal business networks should include but are not limited to, real-time monitoring, detection, and protection mechanisms and technologies. Alerting tools attached to detection processes can give response teams an edge in identifying, mitigating, and containing activities.

Further bolstering internal network defenses with protective measures and mechanisms can completely prevent some forms of attack, such as rogue device sandboxing and logical/physical segregation of networks. Additional access controls should be applied between different networks to prevent unauthorized access and to slow or complicate access through a layered approach.

Record Assets

The organization's Records assets can be either physical or electronic, yet both types of records have similar requirements. Many organizations protect electronic records with encryption, or store backups in secure areas, and protect physical records by locking filing cabinets in secure areas.

However, not much protection of the locations utilized for secure storage within the physical environment is employed by most organizations. Fire can be particularly destructive to physical records, and the use of fire-resistant cabinets is quite common. Water can be equally harmful to paper records, and electronic storage is even more susceptible to water damage, especially in the case of energized storage devices.

System Assets

Organizations design control implementation on Systems to close gaps in protective technologies, mechanisms, and procedures within the organization's infrastructure. Applying the principles of least privilege by removing local administrators and separating privileged accounts from standard accounts can significantly mitigate the potential of some attack vectors by minimalizing the access of unauthorized users to standard accounts.

Careful monitoring of administrative and standard accounts, including log collection and analysis activities, can give security personnel visibility into changes or additions. Tracking changes is essential, as these changes may be precursors to attacks or breaches.

Restricting the use of removable media on systems, such as DVDs, USB drives, and devices, is an additional control that is necessary and effective. Not only do these restrictions bolster the system from a logical hardening standpoint, but they also mitigate another potential attack vector.

Application Assets

For a financial organization, the two critical Applications assets are the Core Financial Application and the Online and Mobile Banking Application. The former functions as arguably the most vital internal system, and the latter functions as a means for consumers to access their monetary assets quickly and

conveniently. Dual-authorization controls for the core financial application are paramount to protecting an organization's assets and should be employed in a documented manner to ensure proper accountability.

Stringent controls for passwords can ensure that consumers have adequate protection measures in place when using online and mobile applications for banking. These controls should include account lockouts, password length and complexity requirements at or above industry standards, and a remembered password history to prevent password reuse. Additionally, the use of multi-factor authentication can grant an added layer of security to sensitive financial transactions executed via the Internet.

Conclusion

Using technology effectively generates risks. The application of proactive measures is, therefore, paramount, especially regarding cybersecurity practices. By mitigating the risk to organizations due to cybersecurity issues, we appropriately ready our defenses for attacks.

This study focuses on the problems of small to medium-sized financial institutions, along with potential mitigating solutions; however, it is by no means a complete study of all financial institutions or their full implementations of cybersecurity programs.

The application of a holistic cybersecurity program can be a daunting set of exercises. Still, such a program can give an organization the means to function in a normal capacity, even in the face of events and incidents that could effectively cripple an unprotected organization.