HSSEDI
Homeland Security Systems Engineering & Development Institute

Prepared for:
Department of Homeland Security

Enterprise Threat Model Technical Report

Cyber Threat Model for a Notional Financial Services Sector Institution

May 2, 2018

Authors:

David B. Fox
Eric I. Arnoth
Clement W. Skorupka
Catherine D. McCollum

The Homeland Security Systems Engineering and Development Institute (HSSEDI)™
Operated by The MITRE Corporation

Approved for Public Release; Distribution Unlimited.
Case Number 18-1613 / DHS reference number 16-J-00184-06

HSSEDI
Homeland Security Systems Engineering & Development Institute

Homeland Security Systems Engineering & Development Institute

The Homeland Security Act of 2002 (Section 305 of PL 107-296, as codified in 6 U.S.C. 185), herein referred to as the "Act," authorizes the Secretary of the Department of Homeland Security (DHS), acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. MITRE Corp. operates the Homeland Security Systems Engineering and Development Institute (HSSEDI) as an FFRDC for DHS under contract HSHQDC-14-D-00006.

The HSSEDI FFRDC provides the government with the necessary systems engineering and development expertise to conduct complex acquisition planning and development; concept exploration, experimentation and evaluation; information technology, communications and cyber security processes, standards, methodologies and protocols; systems architecture and integration; quality and performance review, best practices and performance measures and metrics; and, independent test and evaluation activities. The HSSEDI FFRDC also works with and supports other federal, state, local, tribal, public and private sector organizations that make up the homeland security enterprise. The HSSEDI FFRDC's research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under:

HSHQDC-16-J-00184
Next Generation Cyber Infrastructure (NGCI) Apex Cyber Risk Metrics and Threat Model Assessment

This HSSEDI task order is to enable DHS Science and Technology Directorate (S&T) to facilitate improvement of cybersecurity within the Financial Services Sector (FSS). To support NGCI Apex use cases and provide a common frame of reference for community interaction to supplement institution-specific threat models, HSSEDI developed an integrated suite of threat models identifying attacker methods from the level of a single FSS institution up to FSS systems of systems, and a corresponding cyber wargaming framework linking technical and business views. HSSEDI assessed risk metrics and risk assessment frameworks, provided recommendations toward development of scalable cybersecurity risk metrics to meet the needs of the NGCI Apex program, and developed representations depicting the interdependencies and data flows within the FSS.

The results presented in this report do not necessarily reflect official DHS opinion or policy.

For more information about this publication contact:

Homeland Security Systems Engineering & Development Institute

The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

Email: HSSEDI_info@mitre.org

http://www.mitre.org/HSSEDI

Abstract

The Homeland Security Systems Engineering and Development Institute (HSSEDI) assists the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) in the execution of the Next Generation Cyber Infrastructure (NGCI) Apex program. HSSEDI is developing an integrated suite of cyber threat models for Financial Services Sector (FSS) institutions. The NGCI Apex program will use threat modeling and cyber wargaming to inform the development and evaluation of risk metrics, technology foraging, and the evaluation of how identified technologies could decrease risks. HSSEDI previously developed and populated a high-level framework and threat model tailored to the FSS, as well as an expanded, more detailed threat model. This technical report describes the use of the previously developed extended threat model at the institution level reflecting attacker methods at a level relevant to implementation. This report applies the expanded threat model at the enterprise level. It describes a representative notional FSS institution, identifies where in its enterprise architecture the threat events from the high-level threat model are applicable, and uses a specific scenario to illustrate the use of detailed threat event information.

Key Words

1. Next Generation Cyber Infrastructure (NGCI) Apex program
2. Cyber Threat Models
3. Cyber Threat Framework
4. Enterprise Cybersecurity
5. Financial Services Sector (FSS)

This page intentionally left blank

Table of Contents

List of Figures

List of Tables

1 Introduction

The Next Generation Cyber Infrastructure (NGCI) Apex Program is seeking to accelerate the adoption of innovative and effective cybersecurity technologies in the Financial Services Sector (FSS). As part of that effort, it is developing an integrated suite of cyber threat models applicable to the FSS that can provide a consistent frame of reference complementary to the threat models maintained internally by individual FSS institutions. A high-level threat model [Bodeau 2018], geared toward high-level tasks such as strategic planning or development of scenarios for a tabletop cyber exercise, and an expanded, more detailed threat model [Fox 2018b], which documents potential attack events at a level understandable to both strategic and implementation-level staff, were developed in previous work. The high-level threat model and the expanded threat model, while focused on the FSS, are not enterprise-specific. They are general resources that provide building blocks describing the potential events and behaviors applicable to threat actors seeking to attack any FSS institution. To be used for any specific FSS institution, they would need to be tailored for its particular threat context, business functions, and technical architectures.

This report describes a threat model for a specific, individual FSS enterprise, albeit a hypothetical one. It describes how the high-level and detailed cyber threat models previously developed for FSS institutions are applied and tailored to create a detailed cyber threat model for a specific enterprise. Using a concrete notional example of an FSS institution, it shows how the structure of the enterprise, including its network architecture, business functions, and interfaces, and its sources of risk, including cybersecurity practices, are used to identify which threat events are applicable to which business functions. The resulting example threat model is then used to illustrate how an enterprise-level threat model can be used to create scenarios for that specific enterprise.

1.1 Purpose

This report shows how the detailed cyber threat model can be applied, in conjunction with information about the enterprise's architecture and risks, to identify specific cyber threat scenarios that can be used to support NGCI Apex use cases including:

- Cybersecurity technology foraging
- Cybersecurity test case development for technology validation
- Cyber wargaming scenario development

The example enterprise used in this report to illustrate the tailoring of the threat model is representative of architectures and business functions in FSS institutions but is highly simplified and does not represent any specific, real FSS institution.

1.2 Scope

The focus of this enterprise threat model is on the information technology (IT) environment of an individual enterprise within the FSS, and some of the discussion is tailored to FSS resources and impact. However, it is applicable more broadly. It could be applied to enterprises in other critical infrastructures, with appropriate extension for additional infrastructure-specific aspects such as

unique cyber-physical elements, or to IT environments of large government and private sector enterprises in general.

In the context of the FSS, the expanded threat model presented in this report captures adversary characteristics and potential threat events from the perspective of a single example FSS institution and its external interfaces. It represents the threat directly to that individual institution, including internal, external, and third party risks.

The threat model is limited to potential cyber threats from cyber adversaries to the institution's IT infrastructure. Out of scope are:

- Threats to cyber-physical systems (e.g., physical threats to individual automated teller machines), or threats due to dependencies on non-IT infrastructure (e.g., power or transportation)
- Cybersecurity technologies and mitigations to counter, eliminate, or reduce the risk of threats
- Threats due to fraudulent activities or attempts, rather than cyber attack.

The enterprise threat model in this report is limited to a single institution and its external interfaces. A system-of-systems view of threat models is provided in a companion report [Bodeau 2018b].

1.3 Audience

While this report may be of interest more broadly, its primary audience includes the Department of Homeland Security (DHS) and members of the FSS. Within FSS institutions, it is most relevant to the office of the chief information security officer (CISO), risk management personnel, and technical staff engaged in cybersecurity architecture, engineering, and operations.

The report is written with the assumption that readers have at least moderate familiarity with cybersecurity concepts and terminology.

1.4 Overview of this Document

Section 1 of this report explains its purpose and scope. Section 2 describes the notional FSS institution, its technology environment, business functions, and architecture. Section 3 introduces an institution-specific threat model. Section 4 uses the threat model to develop an institution-specific cyber attack scenario, mapped to both high-level and detailed events of the threat model. Section 5 discusses conclusions. A detailed description of the notional institution's cyber defense capabilities is provided in Appendix A. The complete institution-specific risk profile and high-level threat model are provided in Appendices B and C.

2 Notional Financial Services Sector Enterprise

This section describes a notional example of a financial services sector enterprise, used as the basis for the threat model throughout this report. The notional financial services sector enterprise is highly simplified in many respects compared to the scale and complexity of a large, real-world FSS institution. It is, however, representative of the key business functions and architecture of a large bank, and thus provides a reasonable basis for examining an enterprise-specific threat model.

The aspects of the enterprise relevant to cyber are described in some detail, covering the enterprise's IT architecture, business functions, risk profile, and cyber defense capabilities. While the enterprise is envisioned to have robust and competent cyber defense capabilities, it is not idealized. As in a real-world organization, many of the details of its security configurations and practices reflect decisions made about tradeoffs of cost, benefit, and usability.

This section outlines the following aspects of the notional enterprise:

- business-specific view of enclaves, interfaces, interactions
- network view of data centers, network structure
- risk view of sources of risk to the enterprise
- summary of cybersecurity capabilities and countermeasures

Section 3 then describes the tailoring of the high-level and expanded threat models defined in [Bodeau 2018] and [Fox 2018b] for the notional enterprise.

2.1 Corporate Wide Area Network (WAN) Overview

Figure 1 is a high-level depiction of the entire corporate wide area network (WAN) of the Notional Financial Services Enterprise (NFSE). The WAN consists of many different sites, spread geographically over the Northeast of the United States, connected together through a series of leased lines and virtual connections through telecommunications companies.

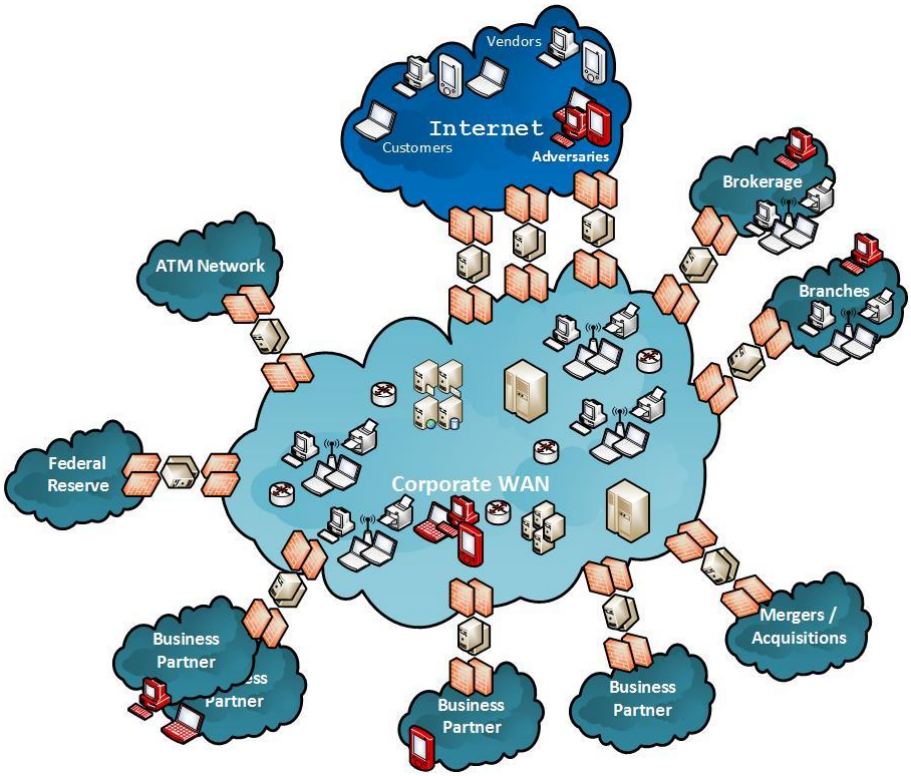

Figure 1. Notional Financial Services Enterprise Wide Area Network

2.1.1 WAN Internal Composition

Different types of sites that make up the WAN include:

- Major data centers
- Minor data centers
- Campuses (non-customer facing)
- Branches (customer facing)
- Smaller offices
- Automated Teller Machine (ATM) sites

Within the WAN, little exists in the way of network segmentation in the form of packet-blocking or inspecting technologies. This lack of security components is a conscious choice of the organization, mainly driven by cost-benefit analysis that deemed the risk was insufficient to warrant the capital or operational expenses.

Many different technologies are deployed throughout the WAN, including the following:

- Desktops
- Mobile devices – laptops, smartphones, tablets
- Servers (dedicated physical or hypervisor installed)
- Network equipment – switches, routers

- Wireless – access points, bridges
- Mainframes
- Storage Area Network (SAN) appliances
- Multifunction printers
- Voice Over Internet Protocol (VoIP) telephony – phones and Private Branch eXchange (PBX) servers
- Industrial Control Systems (ICS) to support building maintenance, heating, and cooling[1]
- Physical security computer systems (badge readers, door locks, etc.)[1]

All told, the NFSE has recently determined that they host a combined total of approximately 300,000 devices that are attached and addressable on their internal network.

In the last few years, the enterprise has adopted a lenient Bring Your Own Device (BYOD) policy that encourages, and in some cases requires, employees to use their own equipment (laptops, phones, and tablets) to conduct enterprise business. The cost savings were considered worth the potential risks, given the other mitigations in place.

2.1.2 WAN External Connectivity

The enterprise WAN has many interfaces to external networks, including the following:

- The Internet
- Dedicated, trusted third parties (business-to-business [B2B] connections, Federal Reserve links, etc.)
- Mergers and acquisitions (i.e., partially trusted companies / subsidiaries in the process of being acquired or divested)

Each connection to an external network is hosted in a strictly controlled and standardized architecture that utilizes different combinations of security controls deemed appropriate for the given risk. Internet connections are considered the highest risk and so have the most security controls implemented. Of lesser risk are the connections to trusted third parties, so they have accordingly fewer security controls implemented. Links to companies and/or subsidiaries undergoing a merger, acquisition, or divestiture have varying degrees of security controls implemented, based in each case upon the current directionality and perceived or assessed risk of the other party.

2.2 Business Enclave View

Figure 2 depicts the relationship between business applications and the network architecture.

[1] While threats to the physical devices and functions of cyber-physical systems are beyond the scope of this threat model, these building access and control systems include IT systems and interconnections that can be either a target of attack or a path via which the enterprise networks can be attacked.

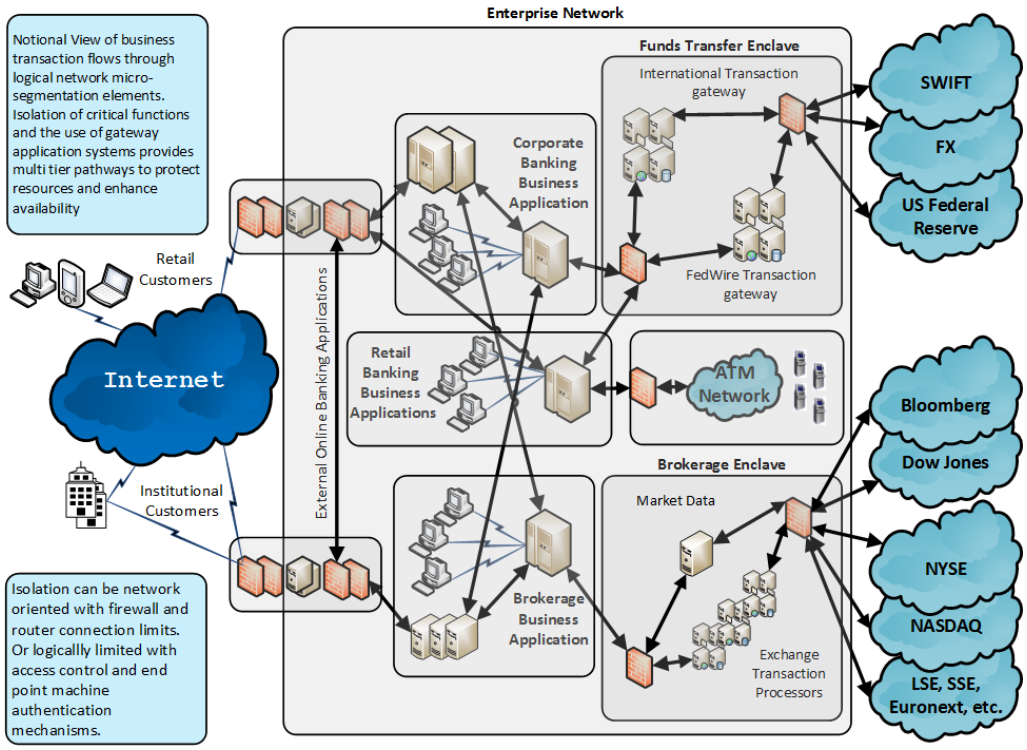

Figure 2. Notional Financial Services Enterprise Business Enclaves and Interfaces

Mapping the described notional financial institution's business enclaves against the Federal Financial Institutions Examination Council (FFIEC) Cyber Assessment Tool (CAT) inherent risk profile [FFIEC 2017] identifies business functional areas of operational risk. These are overlaid on the network and system connectivity to depict a business transactional flow to produce a map of dependencies. Typical mitigating controls and processes, as depicted in Figure 2, are then considered as input to a notional identification of higher risk areas.

Three significant business functions and the interaction of transaction flows are depicted. Personal banking workflows originate from individual customers through internet facing dedicated applications, ATMs, interaction with customer service and branch personnel, and inter-bank transactions. Corporate workflows largely follow the same paths, with the addition of more automated and higher value transaction feeds both through direct network connections and through Internet delivered commercial customer applications.

Backend application processing is used to aggregate transactional flows into external third-party functions. Funds Transfer includes integration with sector utilities such as Society for Worldwide Interbank Financial Telecommunication (SWIFT), Funds eXchange, and governmental central banks (e.g., U.S. Federal Reserve) supporting real-time money transfer, with little recourse for fraudulent or erroneous activity.

ATM networks are isolated to provide security and network priority to customer interaction transactions. These environments remain a target of criminal activity as well, with most of the fraud making use of physical attacks with card skimmers and machine operation hacks. These are often linked to attacks against the banking functions and user access credentials of individual customers and associated endpoint platforms such personal computers (PCs) and mobile phones.

Brokerage processing uses both inbound and outbound third-party functions. Sources for market data that include current pricing, financial news, historical data, and analytic output are actively used for customer pricing and advice. Trade execution is done through other connected institutions, including the New York Stock Exchange (NYSE), NASDAQ, Euronext, and other national and international trading platforms. Additionally, connections to the Internet for open source feeds allowing Broker / Trader analytics are maintained with minimal filtering and high data flows to provide support for business operations, marketing, and direct customer interaction.

Even with mature control frameworks, Funds Transfer, ATMs, and Brokerage operations remain among the highest operational risk environments. These functions provide an ongoing target for both nation-state sponsored advanced persistent threats (APTs) and sophisticated cyber criminal attacks. Funds transfer environments have experienced some of the more notable media-reported hacks, including recent attacks using the SWIFT Financial Services utility. Mechanisms for segregation of business-aligned operational enclaves to support these business functions, including external connection isolation, dedicated transaction filters, dual control process workflows, and multi-factor authentication and access control, have served to reduce the level of risk. But the potential for significant impact, both monetary and reputational, remains high.

To support security, enterprise networks use perimeter methods, such as firewalls, router access control lists (ACLs), and micro-segmentation elements, to provide a protection layer to the business infrastructure. External network traffic is directed through a set of firewalls and dedicated application functionality filters to provide an abstraction from business support systems and data. Additional control points include internal firewalled enclaves to provide stronger protection for availability and integrity. Separation of the three networks for Funds Transfer, Brokerage, and ATM processing using firewalls is depicted.

To provide elements of availability and confidentiality protection of the network traffic, additional isolation occurs using micro-segmentation techniques to segregate network subnets, or class C segments, between production, testing, development, and user systems. This is done with isolated Address Resolution Protocol (ARP) routing or through isolated Virtual Local Area Networks (VLANs).

Further containment relies on logical authentication, authorization, and process controls. User or system-to-system connectivity is further restricted by access permissions through system login and resource access restrictions to specific business application functions. Functions within the application may additionally enforce business process workflows, such as two-person dual controls, based on risk levels of individual transactions.

2.3 Data Center and Network View

This section describes the enterprise's corporate backbone, data centers, and their internal architecture and interfaces.

2.3.1 WAN Architecture

The following diagram depicts the backbone connections of the corporate WAN of the NFSE.

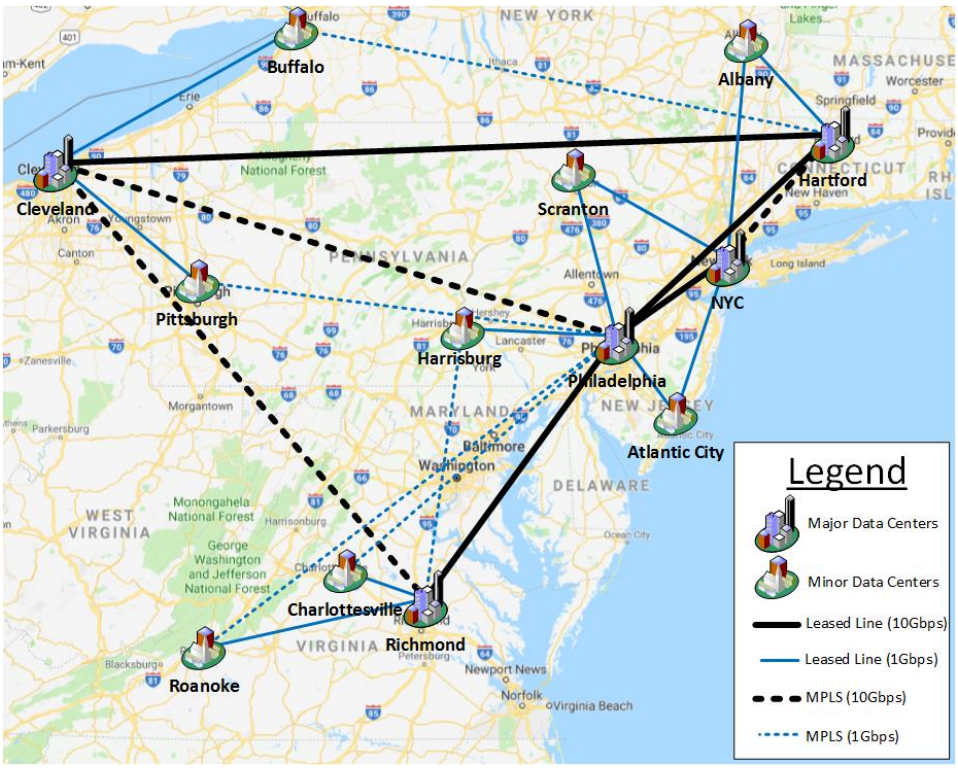

Figure 3. Notional Financial Services Enterprise Wide Area Network Architecture and Backbone Connections

In this diagram, the major and minor data centers are depicted, along with their interconnections. All interconnections were planned with the intention of maximizing high availability while reducing cost. Each major data center has at least one leased line connection to another major data center. Each major data center has at least two connections to another major data center, with less expensive virtual connections being provided by telecommunications provider Multiprotocol Label Switching (MPLS). The data links between major data centers are high bandwidth, carrying 10 Gigabits per second (Gbps). All leased line links were chosen to ensure that if all MPLS links fail, a leased line path will always exist that passes through all major data centers. Where possible, MPLS connections were made on the longer haul lines to improve cost savings.

Each major data center also has connections to at least two different minor data centers, with at least one being a dedicated leased line. Additional connections are likewise supplemented by MPLS as a further cost saving measure. Each minor data center has at least two connections to different major data centers. These links are only 1 Gbps, due to the lower requirements for the applications and components that reside in the minor data centers.

All major and minor data centers are enterprise-owned and managed.

Components of the WAN that are not depicted on this diagram include the following, all of which are connected through the major data centers.

- Campuses and branches
- The ATM network
- Dedicated, trusted third parties (B2B connections, Federal Reserve links, etc.)

- Mergers and Acquisitions (partially trusted companies / subsidiaries in the process of being either acquired or divested)

The minor data centers provide no direct connectivity to other types of enterprise sites but the major data centers.

Also not depicted in the diagram are Internet connections. These all occur at major data centers, or directly at some branch locations.

2.3.2 Major Data Center Architecture

The following diagram illustrates the standard architecture of the major data centers that compose the core of the NFSE's WAN backbone.

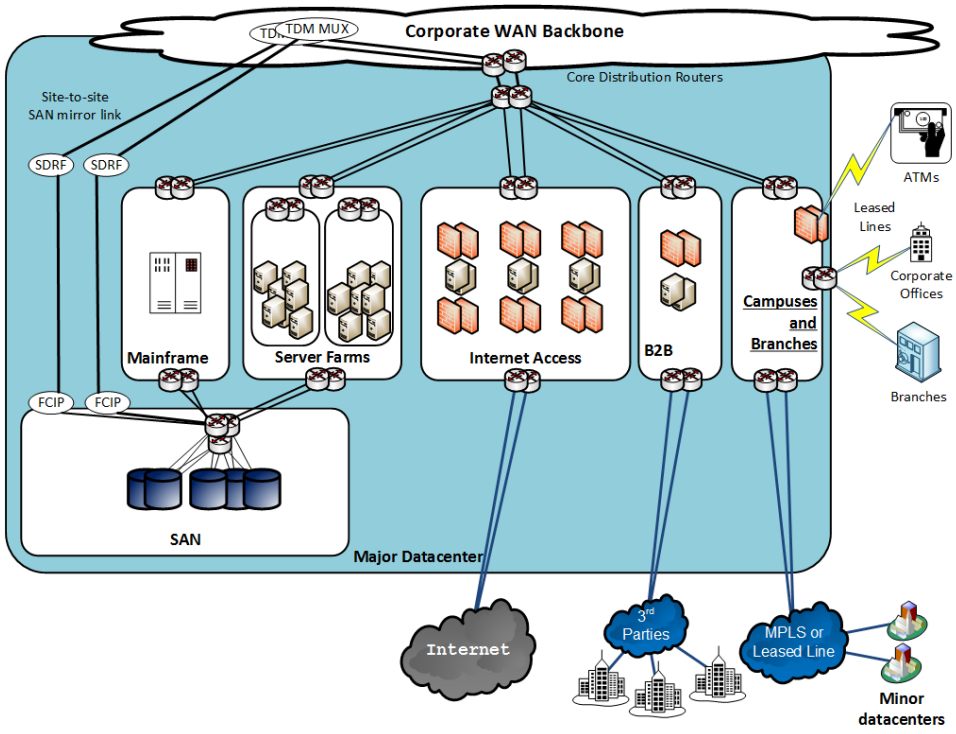

Figure 4. Notional Financial Services Enterprise Major Data Center Architecture

As shown, each data center comprises different types of networks that are dedicated to a particular functionality. While some of the separations are dictated by security concerns (such as Internet and Trusted Third Party), the rest are governed by network architecture best practices to provide the best quality of service and survivability in the case of component or site failures. Except for where firewalls are shown in Figure 4, few network level blocking mechanisms are implemented in any part of the network.

The following subsections explain the components depicted in Figure 4. Details of security controls implemented in each environment can be found in Appendix A.

2.3.2.1 Corporate WAN Backbone

The Corporate WAN backbone is the linkage between major data centers as depicted in Section 2.3.1. Links between data centers are high-throughput and growing, putting strains on the 10

Gbps linkages. The Network Engineering department is currently executing a project to upgrade all major data center lines to 40 Gbps.

2.3.2.2 Server Farms

The Server Farms are common network segments for housing all servers, regardless of business line, or operational support function.

Due to the pervasive use of virtualization to maximize efficiency and cost savings of hardware usage, these networks have additional linkages to the Storage Area Network (SAN) appliance networks. Currently, the NFSE is struggling with the challenges of housing hypervisors and their accompanying high demand for server-to-server communications capacity within data centers originally designed for high server-client communications capacity between the data centers and external networks.

2.3.2.3 Storage Area Network (SAN)

The SAN houses appliances that provide high speed access to massive volumes of disk for use by the server farms. Each major data center has a partner major data center, with the respective facilities' SAN appliances linked through dedicated lines to provide mirroring capability for data written to a disk array in one location.

2.3.2.4 Internet Access

The Internet Access network is protected by strong security controls at its borders and inside of its networks. This environment is isolated from both the Corporate WAN and the Internet by dedicated, stand-alone, physical firewalls. Additional controls are implemented to govern the traffic entering and leaving the enterprise network, as well as to monitor allowed traffic in an attempt to detect hostile activity.

2.3.2.5 Business-to-Business (B2B)

The B2B segment is protected by some security controls, but to a lesser degree than the Internet Access network, due to its role in connecting the NFSE to trusted third parties such as business partners or customers. The Corporate WAN is separated from the links by dedicated, stand-alone, physical firewalls, but few other specialized controls are implemented.

2.3.2.6 Campuses and Branches

The Campus and Branches networks provide WAN connectivity to the facilities other than major data centers, a list that includes minor data centers, campuses, branches, and corporate offices. Connectivity to these various facilities is not secured in any way, and is provided by either dedicated leased lines or virtually through MPLS. The ATM network linkages are also made in this network, but the links are isolated on VLANs and by dedicated firewalls. These firewalls are some of the few examples of internal network segmentation by active security controls.

2.3.2.7 Mainframe

The Mainframe network provides connectivity to the mainframes used for back-end processing. Like the Server farms, this network has direct connections to the SAN networks and does not have any extra security to isolate it from the rest of the Corporate WAN.

2.4 Risk Profile

Assigning risk factors to business functions and organizational units can be useful in helping to focus threat modeling and risk assessment exercises. We perform such an assignment against our notional enterprise in the form of a table derived using the FFIEC CAT's Inherent Risk Profile[2]. Table 1 is a brief sample of a few rows of the table representing the risk profile of the notional financial services enterprise. Due to its size, the complete table is provided in Appendix B.

Table 1. Notional Financial Services Enterprise Risk Profile (Example)

Legend

N	= Not deployed, not planned
Y	= Extensive deployment / use
S	= Select deployment / usage
P	= Pilot program, experimental technology
I	= Incomplete deployment

Category	Factor	Notional Enterprise High-Level Description	Internet	Business-to-Business	Corporate WAN	Corporate Banking	Retail Banking	Brokerage Application	Online Banking	Funds Transfer	ATM Operations	Brokerage Enclave
Technologies and Connection Types	Total number of Internet service provider (ISP) connections (including branch connections)	The five major data centers Some of the branches	Y	S	N	N	N	N	Y	N	N	Y
	Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None exist	N	N	N	N	N	N	N	N	N	N
	Wireless network access	Available universally at all branches and campuses	N	N	Y	N	N	N	N	N	N	Y

The entries in the table are based on the preceding description of the notional financial services enterprise, using values representing reasonable/common practices for each of the risk factors. The relevant risk factors are identified for each of the notional institution's security-relevant business networks and enclaves. Assigning risk factors to the specific business components

[2] https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017_Inherent_Risk_Profile_June2.pdf

allows a more focused and detailed assessment of risk, and construction of relevant, more fine-grained threat scenarios.

The color-coding represents the relative level of deployment or commonality of the practice or element across the organizational business component. Since the practices or elements listed are potential sources of risk, the absence of the practice being deployed is color-coded as green, and its presence to varying degrees as red, orange, or yellow.

As one might imagine, not all risk factors apply equally across an enterprise, though most of the FFIEC risk factors apply to at least one, if not multiple, business networks or enclaves. For example, BYOD practices introduce risk to the brokerage and Corporate WAN (Corporate internal network) components. Administrative access across all business units is another common source of inherent risk.

The analysis indicates that the notional FSS enterprise has a considerable number of risk factors in the brokerage enclave. Section 4 constructs a threat scenario that focuses on that component.

2.5 Cybersecurity Protection and Defense Capabilities

Cybersecurity protection and defense capabilities in place in an enterprise are relevant to potentially narrow the threat events available to an adversary seeking to attack the enterprise. An FSS institution with the business functions identified for the notional enterprise in this report would be regularly challenged by cyber adversaries and would have a robust suite of protection and defense capabilities. This section describes the suite of cybersecurity tools and processes the notional enterprise has, in the following categories:

- **Network.** Some of the core controls implemented by the NFSE are at the network layer. Technologies applied here serve to segment hosts with different purposes and business lines, as well as attempting to prevent and/or detect hostile activity passing to and from the enterprise.
- **Data.** Controls applied in storage and transmission of data are implemented to help the NFSE ensure confidentiality and integrity.
- **Host.** Software used on the host layer are implemented in an attempt to prevent and detect malicious activity through a variety of means.
- **Application.** These controls are used to ensure confidentiality of data and protect against compromise of user accounts.
- **Security management.** Due to the wide array of technologies deployed throughout the NFSE, a centralized system to collect and analyze the data generated by these security components is needed. These facilities serve as the heart of the enterprise's ability to detect malicious activity.
- **Processes.** While technology controls are important, a key part of the NFSE's security is provided through the processes conducted by its employees. These processes encompass many different areas and parts of the enterprise, touching almost all operations in one way or another.

- **Architecture.** The fundamental design of the network and applications that live within it serves as a form of control, laying the foundation of the other segmentations implemented by other control layers.
- **Services.** Services provided by third-party companies are used by the NFSE to augment their security, for purposes such as providing intelligence about potential adversaries and providing additional protections against certain types of attacks.

A brief description of each is given in this section. Appendix A provides a mapping of the defensive capabilities to the notional financial services enterprise's specific networks and business enclaves.

2.5.1 Network

The following are network-layer controls implemented by the NFSE.

- **Routers.** Most commercial routers provide the capability to block traffic based upon source and/or destination Internet Protocol (IP) address and/or application port in the form of ACLs. The NFSE employs ACLs on its border routers to prohibit some inbound communications on its perimeter, relieving the firewalls of some capacity requirements. Additionally, the backbone routers block a few ports and protocols that have been used in the past by malicious software to cause harm to the enterprise. The enterprise also generates netflow reports from some of its routers to provide raw data for its security analytics.
- **Firewalls.** Dedicated firewall devices are employed at the borders of the NFSE's network with the various third parties. These devices consist of a mixture of classic stateful firewalls and newer next generation firewalls (NGFWs) that do deep packet inspection. Due to the high cost of the NGFW devices, not all networks protected by firewalls are converted.
- **Virtual Private Network (VPN) Concentrators.** To facilitate secure remote connectivity by employees and some third parties, dedicated VPN concentrator appliances are deployed into the Internet facilities at every major data center. These devices provide an authenticated, encrypted tunnel from authorized laptops, mobile devices, and some remote sites to provide IP routing back into the corporate WAN of the NFSE.
- **Intrusion Detection and Prevention Systems (IDPSs).** IDPSs monitor traffic and look for data patterns that may indicate an attack or a successful compromise. A mixture of out-of-band, packet intrusion detection systems (IDSs) for detection only, and inline intrusion prevention systems (IPSs) for blocking attacks, are deployed at all Internet Facilities and a few select B2B links. The backbone links between major data centers also have deployments, though these devices are very limited in what they watch for, due to extremely high performance requirements.
- **Sandboxes.** Sandbox technology watches for potentially hostile files and attempts to open or execute these in instrumented virtual machines that are contained in an isolated appliance. The intent is to identify attacks targeting client-side software within the NFSE's network. Although this technology has shown some value, its high cost has prevented the enterprise from deploying more widely to all Internet links.

- **Outbound Web Proxies.** In order to monitor web requests to the Internet and filter attempts to connect to improper sites, the NFSE forces all outbound traffic through a series of web proxies. These proxies log all connections, authenticating individual users via their desktop operating systems to provide accountability. Blacklists of banned Uniform Resource Locators (URLs) are updated regularly by both the company that sells and supports the proxies and through use of open source content provided by the security community.
- **Reverse Proxies.** For the purposes of both load balancing and enhanced security, some of the NFSE's Internet-facing applications utilize reverse proxies, which provide a unified front-end for server farms hosted in the Internet facilities of the major data centers. These devices provide limited capabilities to monitor inbound requests to the web applications, attempting to detect and/or prevent simplistic attacks.
- **Sinkholes.** As part of the enforcement mechanism to force all outbound corporate communications through the outbound web proxies, the enterprise WAN does not have a default route to the Internet. Instead, if any communications are destined to addresses that are not part of the corporate WAN, they are instead routed towards a sinkhole router. This router summarily drops these packets and reports all traffic in netflow transmissions to the security management facilities. By doing this, the NFSE can identify both misconfigured applications and malicious software that was not designed to use the web proxies.
- **Netflow Analytics.** Various routers throughout the enterprise transmit reports of the traffic they pass, consisting of which machines are talking to each other, which application ports they are using to do so, and how much data was transmitted each way. By data mining this content, the Security Operations Center (SOC) is able to detect some hostile activity, including attempts by compromised assets to phone home, the build up to a denial of service (DoS) attack at the Internet links, and suspicious peer-to-peer communications within the enterprise.
- **Packet Recorders.** As part of the forensic suite to better identify whether an attack or breach has been attempted or accomplished, dedicated appliances have been deployed at the Internet Facilities of the major data centers. These appliances not only record and store all communications to and from the enterprise, but they also provide a robust user interface to facilitate searching the massive amount of data gathered. Due to capacity limitations and costs, the devices typically can only hold three weeks' worth of data.
- **Distributed Denial of Service (DDoS) Prevention.** Due to attempts in the past to impact business operations of the NFSE on the Internet, the enterprise has purchased and deployed dedicated appliances that attempt to mitigate denial of service attacks that target their web applications. Larger attacks that could saturate the Internet connections themselves need to be mitigated by a cloud service provider, with which the enterprise contracts for service. (See Section 2.5.8)
- **Compromise Detection.** Appliances that watch for known traffic patterns indicative of traffic from compromised assets to command and control (C2) servers on the Internet have been deployed at the Internet facilities of the NFSE. These devices help the

enterprise determine some cases when their perimeter has been breached but do not detect all variations of C2 traffic.

- **Web Application Firewalls (WAFs).** These dedicated devices sit in front of some of the web applications hosted in the NFSE's Internet Facilities to observe inbound requests from the Internet. They watch for data patterns that may indicate attempts to compromise the enterprise's web applications and can either block such attempts or alert on them.
- **Email Antivirus.** All email servers that provide email within the NFSE or provide email services to the Internet are equipped with software that looks for data patterns that may indicate known malware is being transmitted. When a successful detection occurs, the offending message is blocked and a bounce message is sent to the sender.
- **Domain Name System (DNS) Log Monitoring.** To aid in the detection of compromised assets within the enterprise, outbound DNS requests are monitored and data-mined to detect known hostile patterns.

2.5.2 Data

The following data layer controls are implemented by the NFSE.

- **Data Loss Prevention (DLP).** In order to prevent either the intentional or accidental transmission of customers' Personally Identifiable Information (PII), the NFSE has deployed DLP software that monitors outbound email for artifacts such as social security numbers. When a successful detection occurs, the offending message is blocked and a bounce message is sent to the sender.
- **Encryption.** To ensure confidentiality of sensitive communications, the NFSE has deployed a number of different encryption solutions for communications used. Employees have the option of signing up for email encryption capabilities, which are implemented through special desktop software. All enterprise applications that work with sensitive information or customer PII are required to encrypt their traffic in transmission or at rest. All enterprise laptops' hard disks are encrypted by a third party product, to protect against data theft if the device is stolen or lost.

2.5.3 Host

The following host layer controls are implemented by the NFSE.

- **Antivirus.** All Windows-based desktops, laptops, and servers are required to run antivirus software. The NFSE has standardized on a solution from a major security vendor, and has centralized the management of the software and its weekly updates for new signatures to detect new malware.
- **Host-based Intrusion Prevention System (HIPS).** The NFSE has acquired HIPS software that can prevent some attacks targeting computers. Although this software has shown some evidence of success, it also tends to break legitimate applications. As a result, NFSE's deployment of HIPS is limited to high-risk servers.
- **File Integrity Monitoring Software.** In an attempt to detect compromises, some servers are equipped with software to detect if adversaries replace legitimate system programs with malicious ones. This is often done after a system is compromised. The malicious

programs tend to serve multiple purposes, such as to provide illicit access and to hide the presence of the adversary by lying to legitimate users about what is happening on the system.

- **Automated Patch Management and Distribution System.** To ensure that all security patches are applied to affected systems on the corporate WAN, the NFSE has purchased and deployed software that will deploy and install updates to both the operating systems and the applications.
- **Sandboxing of Applications.** A new class of technologies, application sandboxes, attempt to prevent system compromise by wrapping each program in a container that attempts to isolate the rest of the system from any individual breach. Although this technology shows promise, it is also extremely invasive. The NFSE is conducting a pilot program to assess whether the costs and impact are worth the potential risk mitigation.
- **Whitelisting.** Attempts have been made in the security community to implement application whitelisting, so that only trusted programs are allowed to run on a system. While this technique has great promise to reduce the ability of adversaries to function after compromising a foothold system, the NFSE expects that it may severely limit the ability of the various business lines to do their work effectively and efficiently by creating a bottleneck for all IT development. A pilot program is being performed to assess the potential impact to business operations.
- **Browser Security.** Due to web browsers being a regular target of advanced adversaries, a special effort is made to standardize enterprise use of browsers, enhance their security through plug-ins, and keep them to the latest patch levels. Due to the varying and divergent demands of each business line, however, this effort has shown limited success.
- **Host Configuration Management.** In order to enforce some uniformity in how the various servers, desktops, and laptops within the NFSE are deployed, software has been purchased and rolled out that attempts to standardize the configurations of the various systems. Due to the varying and divergent demands of the each business line, however, this effort has shown limited success.

2.5.4 Application

The following application layer controls are implemented by the NFSE.

- **Multi-factor Authentication.** To enhance security, high risk applications and administrative interfaces to various IT platforms have been configured to use token-based authentication, thus implementing one-time passwords. In addition, Public Key Infrastructure (PKI) has been rolled out to provide application layer, mutual authentication between clients, servers, and middleware components.
- **Single Sign-On (SSO) authentication.** To reduce the likelihood of accounts being hijacked and improve accountability, all web-based applications have been forced to implement the corporate standard SSO solution. As a consequence, all employees only authenticate once to their desktop and their identity is subsequently propagated to all internal applications that they use.

2.5.5 Security Management

The following security management controls are implemented by the NFSE.

- **Security Incident and Event Manager (SIEM).** The SIEM provides log and alert aggregation for all security technologies on the network, host, and data layers. The NFSE has a contract with a major security vendor that provides world-class software and appliances for this purpose, and has been very successful in rolling it out. The effort to make use of the data in meaningful correlation rules has been somewhat lacking, but a continuous project is underway to improve the situation, with the help of contractors provided by the security vendor.
- **Log Analytics.** In order to provide additional intelligence for all of the logs collected, analytic appliances get copies of log data sent to the SIEM. These specialized appliances also collect non-security data, including logs from servers and applications. Using the enhanced analytic engine in these appliances, the NFSE is able to data mine for unusual activities or Indicators Of Compromise (IOCs) that they learn about.

2.5.6 Processes

The following process controls are implemented by the NFSE.

- **Office of the Chief Information Security Officer (CISO).** The CISO function provides governance by establishing management structure, assignment of responsibilities and authority, overseeing the development of a corporate policy or risk tolerance baseline, review of non-compliance acceptance, tracking of metrics and trends in implementation effectiveness, and communication with other corporate and business management.
- **Security Operations Center (SOC).** The SOC is a centralized part of the NFSE's cybersecurity division with operational responsibility for monitoring all alerts and logs generated by the enterprise's devices. They are the primary users of the Security Management tools and are responsible for reporting on any attempts to compromise the enterprise's systems or on successful breaches. They are also responsible for ensuring that content updates for systems like IDPS and Antivirus are deployed in a timely fashion.
- **Incident Handling.** A dedicated team of trained, certified, and experienced incident handlers is a part of the cybersecurity division. These individuals are well versed in how to respond to a live incident and collect evidence in a fashion that will comply with chain of custody requirements in the case of any legal proceedings that may arise. They have connections with both federal and local law enforcement and have built an extensive network of relationships in many different areas of the company to facilitate their response process.
- **Compliance Monitoring.** A variety of compliance organizations within the NFSE are responsible for ensuring all businesses and IT functions, such as engineering, operations, and administration, are operating in accordance with all laws, regulations, and enterprise policies. These organizations report to the management chain of the organization they are responsible for helping. Each group prepares for any audits that they are required to go

through, as well as performing continuous monitoring of all operations and activities to ensure compliance.

- **Internal Audit.** The NFSE has an internal, centralized audit organization that regularly reviews business, operations, and technology implementations within the enterprise. This department reports directly to the enterprise's Board of Directors and is accountable for assessing the effectiveness of risk management processes and compliance with legal and regulatory requirements.
- **External Audit.** Due to legal and regulatory requirements, the NFSE is regularly subjected to audits by external entities. Some of these audits are done by private companies under contract to the NFSE; others are done by the relevant government regulators. Each of these audits reviews aspects of the enterprise's operation to ensure compliance with governing laws and regulations, as well as prudent management of risk.
- **Supply Chain Risk Management.** To reduce the risk of compromise being introduced by its dependence on services and computer systems purchased to run their business, the NFSE makes efforts to verify that their suppliers are trustworthy, by selective assessments, review of business stability (e.g., Dunn & Bradstreet), consulting news, governmental reports, and their threat intelligence vendors. (See Section 2.5.8)
- **Training.** To ensure their employees are current on the latest threats faced and technologies being implemented, the enterprise has a training regime with both internal and external facilities. Although not all employees are able to attend training every year due to cost, a 'train-the-trainers' program is instituted to attempt to promulgate the new knowledge to all stakeholders after each set of employees are able to attend training.
- **Vulnerability Remediation Management.** Due to the constant flow of new vulnerabilities in software and services that are published worldwide, the NFSE has a standing process and an organization dedicated to monitoring the stream of reports and determining when any given vulnerability presents significant risk to the enterprise. This organization is responsible for governing and driving the security patch schedule, and performing a triage function to ensure the highest risk items are addressed in the shortest period of time.
- **Asset Baseline and Configuration Monitors.** To ensure consistency and compliance to published standards within the enterprise, servers, desktops, and laptops are equipped with software to monitor their configuration. Violations are reported to Compliance so that the open issues can be driven to remediation.
- **Vulnerability Scanner.** In order to determine compliance with the enterprise patch schedule, network and host scans are regularly performed using commercial software that specializes in identifying vulnerable services and applications. Violations are reported to management to help drive application of patches to delinquent systems.
- **Penetration Testing.** To obtain an end-to-end evaluation of the NFSE's security posture, the enterprise regularly contracts with external firms that specialize in penetration testing. These firms conduct actual attacks against the enterprise's infrastructure, within defined scopes and time-frames, both to test the effectiveness of the installed defenses and the ability of the SOC to react to any observed attacks.

- **Change Management.** An established and deeply entrenched change management process and culture are instilled in the NFSE. No change in production is made without extensive planning, testing, and quality assurance review. Changes are only authorized through an official request system, which requires sign-off from all potentially affected parties before a change is executed. Changes are scheduled in a given, off-hours green zone, and each change must have formal test plans and roll-back procedures, in case the change does not go as intended.
- **Awareness Training.** Due to the role that users can play in security, a regular awareness training program exists within the NFSE. This program serves to communicate to users what are best practices, what to watch for, and what enterprise policy is regarding all aspects of cybersecurity. The program also educates employees on the enterprise's fiduciary, regulatory, and legal obligations.

2.5.7 Architecture

The NFSE implements segmentation of enclaves, using firewalls, ACLs, and routing in its architecture. High-risk components of the network are isolated from one another to varying degrees by different network technologies. This isolation reduces the overall risk faced by the enterprise by limiting access.

2.5.8 Services

The following security services are used by the NFSE.

- **DDoS Mitigation**. When a significant DDoS attack occurs, the NFSE works with a DDoS mitigation service provider that it has contracted with to redirect inbound traffic through the cloud facilities on its way to the enterprise's own Internet Facilities. The cloud protection provides additional capacity and actively scrubs the hostile traffic to reduce the final load that reaches the enterprise's Internet-facing business applications.
- **Threat Intelligence**. The SOC obtains a regular feed of IOCs, known hostile domains and IP address blocks, as well as custom signatures from several threat intelligence vendors that the NFSE has contracts with. These data feeds are used in part to data-mine the logs and alerts collected in the security management suite, as well as to deploy custom detections to the various defensive tools used by the enterprise.

3 High-Level Enterprise Threat Model

In [Bodeau 2018], we developed a framework of high-level cyber threat events that incorporates elements from National Institute of Standards and Technology (NIST) SP 800-30, "Guide for Conducting Risk Assessments" [NIST 2012] and the Cyber Threat Framework [ODNI 2017].

We apply this high-level threat framework to our notional enterprise, in order to identify threat events relevant to the enterprise, and specify which components of the enterprise might be affected by those threat events.

Due to its size, the complete mapping of high-level threat events to the notional financial service enterprise's networks and business enclaves is provided in Appendix C. Table 2 provides a representative excerpt showing the format used to represent the mapping. It lists the threat events, categorized by the cyber attack lifecycle (CAL) phase [NIST 2012], and identifies the attack vector by which the activity could take effect. It considers the applicability of each threat event with respect to the different networks and business enclaves of the notional enterprise. A threat event marked "Y" in the column for a particular network or business enclave, and shaded red, is relevant within that network or business enclave. A threat event marked "N" and shaded green is not relevant there. The relevance of a threat event may depend on technologies that are used in the network or business enclave, as well as interfaces to which it connects.

Table 2. Mapping of High-Level Threat Events to Enterprise Networks and Business Functions (Example)

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Internet	Business-to-Business	Corporate WAN	Online Banking	Corporate Banking	Retail Banking	ATM Operations	Funds Transfer	Brokerage Operations
Recon	Perform perimeter network reconnaissance/ scanning.	External network connection	Interception	Y	Y	N	N	N	N	N	N	Y
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	N	N	Y	Y	Y	Y	Y	Y	Y
Weaponize	Craft phishing attacks.	External network connection, email	(no immediate effects)	N	N	Y	Y	Y	Y	N	N	Y
Weaponize	Craft psychological manipulation attacks on key staff.	Social media interactions	(no immediate effects)	N	N	Y	Y	Y	Y	N	Y	Y

This mapping of threat events to business networks and enclaves can be used as input to threat modeling and scenario building. For example, one can choose a particular business network or enclave such as the brokerage enclave, and then build a threat scenario by choosing high-level threat activities that are applicable to that business enclave (such as "Deliver targeted malware for control of internal systems and exfiltration of data" via the attack vector "Internal network" to the "Brokerage Enclave"). One could also perform a more exhaustive modeling exercise by considering all applicable threat events for each business component.

After identifying the relevant high-level threat events for a given scenario, one can then perform a detailed level analysis of activity by employing the detailed threat event table, as developed in the earlier expanded threat model report [Fox 2018b].

A full threat modeling exercise would consider the combination of the inherent risk of different business and IT practices, in conjunction with the in-place defenses and mitigations, to further reduce the set of applicable threat events to consider. For example, a ransomware campaign that propagates via exploits against older known vulnerabilities is less of a threat if enterprise systems are patched in a timely and thorough fashion.

Section 4 constructs a relevant threat scenario focused on the brokerage enclave, employing threat events that are applicable to that enclave. As reflected in Table 7Table 1, this enclave has several risk factors, and residual risk that remains even after consideration of mitigations that are in place. Brokers working in this enclave, by the nature of their work, need access to both critical internal applications such as the trading application, and to many external information sources from the Internet and private communications from customers. Therefore, this is a high-value target for potential attackers. This scenario, and others like it, could be used to inform gap analysis and suggest detection and mitigation strategies or opportunities for new technology to improve the enterprise's cybersecurity posture.

4 Attack Scenario

Section 2 detailed a notional financial services institution with several business functions that represent higher risk operational areas. The business function mapping is used to identify relational trust and dependency areas as transactions are processed in normal day-to-day operations in these identified areas. From these mappings, a set of typically used cyber defenses are identified that are intended to mitigate risk from cyber attacks.

This section uses the derived applicability scores to support development of a realistic attack scenario against a threat model and technology and operations constructs of the identified business unit producing impacted subsections of the overall enterprise threat model described in Section 3. The exercise uses examples of known APT tactics and their attempts to avoid detection through multi-stage compromise of technology trust relationships and minimized execution artifacts as detailed in the Adversary Tactics Techniques and Common Knowledge ™ (ATT&CK ™) [MITRE 2015], Common Attack Pattern Enumeration and Classification™ (CAPEC™) [MITRE 2016], and cloud security frameworks [Cloud Security Alliance 2016].

The purpose is to show an illustrative example of a scenario that can subsequently be used to trace cyber defensive technology and processes to assess their effectiveness against a sophisticated adversary. The methodology could be reused to cover other aspects of cyber threats, but they are outside the scope of this report. The results of this work would support informed choices in acquisition of new solutions or identification of gaps in existing coverage.

4.1 High-Level Scenario Description

In the following scenario, a user endpoint in a brokerage enclave is compromised, and that endpoint is then used as a stepping stone to conduct an attack against a middleware server that queues transactions for a trading application.

There are two actors in this scenario. An initial criminal attacker exploits a website frequently visited by brokers and others involved in the financial sector, with the goal of compromising user systems as targets of opportunity. A broker from our notional enterprise visits the site, and their browser downloads a general purpose trojan. The malware establishes a command and control channel and is then able to provide an entry point into the enterprise.

The first actor, realizing the potential value of this compromised system, then sells access to this system on the black market to a second adversary. The second adversary is more advanced and specializes in cyber-enabled theft involving financial transactions. The new actor leverages access to the endpoint, conducts reconnaissance, and moves laterally to extend their foothold for a deeper persistence. Having established a fixed presence in the victim network, the actor conducts additional discovery to identify a middleware server that can be further compromised. The attacker employs a zero-day exploit to compromise the middleware application, and injects code that allows them to hold the transactions of specific stocks in the queue. The attacker then releases a news article detrimental to a given company to social media, driving the stock price lower, in order to conduct trades in front of the stalled transaction and derive profit from the trades.

The phases of the attack are summarized in Table 3.

Table 3. Example Attack Scenario: Attack Phases

Attack Phase	Description
1	Compromise of "watering hole" website.
2	Trusted user visits watering hole site compromising endpoint system in trusted enclave.
2a	General purpose trojan downloaded and installed,
2b	Malware establishes C2 channel.
3	Initial actor sells access to advanced/specialty actor on black market.
4	New actor leverages endpoint access, conducts reconnaissance and lateral movement. Identifies middleware server target.
5	Zero-day exploit delivered, compromises application, malcode installed to control transaction process queue.
6	News item released with intent to drive down stock price.
7	Attacker profits by making trades taking advantage of stalled institution's trade.

In Table 4, the different phases of the attack are mapped to a selection of high-level threat events used to carry them out. Note that the transaction between the first and second criminal actor is not an event covered by the high-level events in the threat scenario.

Table 4. Example Attack Scenario: High-level Threat Events

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Attack Phase
Weaponize	Craft psychological manipulation attacks on key staff.	Social media interactions	(no immediate effects)	Phase 6
Weaponize	Compromise systems in another organization to establish a presence in the supply chain.	Supply chain	(no immediate effects)	Phase 1
Deliver	Deliver known malware to internal organizational information systems (e.g., virus via email). (See Cyber Threat Framework [CTF]: Interact with intended victim)	External network connection, email	Corruption, Modification, or Insertion	Phase 2a
Deliver	Deliver modified malware to internal organizational information systems. (See CTF: Interact with intended victim)	Internal network, authorized actions of non-privileged user, authorized actions of privileged user, device port (e.g., removable media)	Corruption, Modification, or Insertion	Phase 2a

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Attack Phase
Exploit or Control	Exploit recently discovered vulnerabilities. (See ATT&CK: Lateral Movement)	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Phase 5
Control	Acquire privileges associated with a user account, process, service, or domain. (See ATT&CK: Credential Access)	Internal network, internal shared or infrastructure services	Unauthorized use	Phase 4
Control	Modify or increase privileges associated with a user account, process, service, or domain. (See ATT&CK: Privilege Escalation)	Internal network, internal shared or infrastructure services	Modification or Insertion	Phase 4
Control	Exploit vulnerabilities on internal organizational information systems. (See ATT&CK: Lateral Movement)	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Phase 4
Control	Exploit vulnerabilities using zero-day attacks. (See ATT&CK: Lateral Movement)	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Phase 5
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Phase 7
Control	Establish command and control (C2) channels to malware or compromised components. (See ATT&CK: Command and Control)	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Phase 2b

4.2 Detailed Scenario

Table 5 maps the attack phases and high-level threat events identified in Section 4.1 to detailed threat events drawn from [Fox 2018b] (at the level of ATT&CK and CAPEC) to illustrate adversarial actions against weaknesses in commonly deployed business architectures. They leverage techniques that appear to be part of a normal support or business function activity.

Table 5. Attack Scenario Mapped to Detailed Threat Events

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Attack Phase	Detailed Threat Model
Weaponize	Compromise systems in another organization to establish a presence in the supply chain.	Supply chain	Phase 1	"Targeted client-side exploitation"-PRE-ATT&CK
Deliver	Deliver known malware to internal organizational information systems (e.g., virus via email). (See CTF: Interact with intended victim)	External network connection, email	Phase 2a	Unconditional client-side exploitation/Injected Website/Driveby-PRE-ATT&CK
Deliver	Deliver modified malware to internal organizational information systems. (See CTF: Interact with intended victim)	Internal network, authorized actions of non-privileged user, authorized actions of privileged user, device port (e.g., removable media)	Phase 2a	Unconditional client-side exploitation/Injected Website/Driveby-PRE-ATT&CK
Control	Establish command and control (C2) channels to malware or compromised components. (See ATT&CK: Command and Control)	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Phase 2b	Standard Application Layer Protocol-ATT&CK
Control	Acquire privileges associated with a user account, process, service, or domain. (See ATT&CK: Credential Access)	Internal network, internal shared or infrastructure services	Phase 4	Exploit Vulnerability-ATT&CK
Control	Modify or increase privileges associated with a user account, process, service, or domain. (See ATT&CK: Privilege Escalation)	Internal network, internal shared or infrastructure services	Phase 4	Exploitation of Trusted Credentials-CAPEC Exploiting Trust in Client-CAPEC
Control	Exploit vulnerabilities on internal organizational information systems. (See ATT&CK: Lateral Movement)	External network connection, trusted or partner network connection, internal network	Phase 4	Create Account-ATT&CK Privilege Escalation-CAPEC
Control	Exploit vulnerabilities using zero-day attacks.	External network connection, trusted or	Phase 5	Exploit Vulnerability-ATT&CK

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Attack Phase	Detailed Threat Model
	(See ATT&CK: Lateral Movement)	partner network connection, internal network, mobile or transiently connected devices		API Manipulation-CAPEC Buffer Manipulation-CAPEC Code Injection-CAPEC Command Injection-CAPEC Exploiting Trust in Client-CAPEC
Weaponize	Craft psychological manipulation attacks on key staff.	Social media interactions	Phase 6	N/A
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Phase 7	Scheduled Task-ATT&CK Command Injection-CAPEC Fault Injection-CAPEC Functionality Misuse-CAPEC Local Execution of Code-CAPEC Malicious Logic Insertion-CAPEC

Initial compromise steps are often end user-generated activities. In this scenario, the compromise of a commercial website to target specific industries is used to present the user with the opportunity to take an action that installs malicious software (malware) on their machine. This is commonly presented as an update to a utility such as Flash or a masquerade of a function of other installed software requiring a user to "click" an approval. This activity is expressed as "PRE-ATT&CK: Targeted client-side exploitation" in Table 5, in row 1.

Each step in the high-level scenario is mapped to the APT tactics, techniques, and procedures (TTP) activity. C2 channels use apparent web traffic to hide their communication with the adversary. In the described scenario, access to the compromised machine is then sold on the black market (e.g., in an exchange on the Dark Web) to a criminal organization with advanced resources to carry out technical attacks that are more focused and difficult.

This C2 channel is then used to deliver additional payloads of software. Local privilege escalation is considered lower risk, and patches may be deferred to allow testing of business software. Once administrator-type access is obtained, extraction of cached credentials is possible without network communications that could be detected by security tools such as IDS.

Once a Windows Domain Account credential has been compromised, logins to other endpoints look like normal help desk or system administrator activity and can provide entry points for horizontal movement into application infrastructure, providing additional channels for attack resiliency. Zero-day, or previously unknown, exploits are often brought in the same way and can be used to establish access to software functions on the target system. In this scenario, we used the message queueing system to delay certain transactions and deliver data to the attacker, who then uses the information to trade within an exchange in front of a market move event to effectively support an insider trade transaction to their financial advantage.

4.3 Discussion

In this report, a highly complex and detailed threat model was readily analyzed to identify threat vectors that would come into play in a given scenario with a given enterprise that has known attributes and risks inherent in its IT platform.

The application of the high-level and expanded threat models to a hypothetical attack scenario has a variety of uses for financial institutions. First and foremost, the enterprise can use these methods to evaluate their existing defenses and identify gaps.

As demonstrated in Table 6 in Appendix A, the defensive suite of an enterprise can be mapped against its high-level network topology and business lines. The defensive suite can be mapped against the threat events to identify how and whether they are mitigated by tools and processes in the defensive suite. By doing this, a thorough and detailed analysis can be performed to identify the gaps in the current defensive suite. Threat events that are not mitigated (or are only partially mitigated) represent residual risk and pose opportunities that could be exploited by an adversary in an attack scenario. Identification of such gaps through analysis of attack scenarios and threat vectors could then be used to guide technology foraging to bolster the enterprise's defensive posture.

This type of analysis also has benefits for testing of new candidate tools for the defensive suite. Such testing can be arduous, due to the extensive range of types of hostile activity that any given tool may be tasked with detecting and or mitigating. Identifying and characterizing the enterprise's high-risk applications and defensive suite, and using the threat model to identify likely attack scenarios can allow test plans to be targeted to the most relevant elements.

While only a single example scenario was constructed in this report, an enterprise using this process of threat-model analysis would need to develop additional scenarios, each with a different selection of threat vectors from the larger, comprehensive list that was documented in [Fox 2018b]. Ideally, enterprises should work towards building a comprehensive suite of scenarios and models to account for the major threats that they face. Variations on each threat scenario could also be outlined to look at how well the defensive suite measures up in different circumstances. When new attack methods become known, they can be examined in the context of existing and new scenarios to determine what countermeasures are needed and where.

Finally, based upon one or more of the scenarios developed and analyzed, it would be possible for financial institutions to design wargames to test in practice whether the defensive tools and processes would be capable of detecting and/or mitigating the attack. Execution of such wargames would be valuable in validating or disproving assessments made in the analytical threat modeling and control alignments described above. Using the results of the wargames, an iterative process could be established that would better inform future versions of the threat models and scenarios, to further increase fidelity and identify new threat vectors and scenarios.

5 Conclusion and Next Steps

In this document, the previously developed NGCI Apex threat modeling framework [Bodeau 2018, Fox 2018b] was applied to a notional financial enterprise's traditionally higher risk business functions. To facilitate this exercise, the fictitious enterprise was presented in detail, documenting business functions, transaction flows, and utilized network segments. How the businesses use the technologies to operate within the defined networks was outlined, with demonstrations of interdependencies and inherent risks. The defensive suite of tools and processes was also presented.

This detailed description of a fictional institution was then used to demonstrate how the threat modeling framework can be used to develop an attack scenario for that institution. The institution could use such an attack scenario in cyber wargaming, technology foraging, test scenario development, and risk analysis. To develop the attack scenario, the FFIEC's Risk Factor Table from the CAT [FFIEC 2017] was applied to the individual components of the enterprise. This illustrated how different risk factors can affect different enterprise components. Subsequently, the threat events defined in the high-level threat model were applied to the notional enterprise, mapping relevant threat events to the specific network and business enclave components. A specific threat scenario was then presented and focused on an attack targeting a particular business and network enclave. The attack in this scenario described both high-level threat events and representative detailed level threat events, based on the threat events provided in [Fox 2018b].

5.1 Results

Using a notional FSS institution as an example, this framework and methodology showed how it is possible to assess the effectiveness of existing controls and identify gaps that the enterprise may want to minimize or eliminate by enhancing the existing controls.

The following resulted from applying the threat modeling framework to the notional institution:

- The identification of the business functions, technology environment, network architecture, and interfaces of the notional FSS institution showed how risk factors affect different enterprise components to different degrees. This can help to structure and prioritize risk analysis.
- Similarly, the analysis of the threat events in conjunction with the specific elements of the notional FSS institution's architecture and business functions illustrated that different threat events are relevant to different enterprise components. This can inform and help structure and prioritize threat modeling studies.
- A plausible threat scenario was developed that was informed by the risk factors and relevant threat events for a component of the enterprise.
- A relatively compact set of specific, detailed attack techniques was identified for the scenario by filtering the mapping of high-level threat events and detailed level attack techniques based on the business components and technology environment to produce a subset of factors to be considered. This is a useful reduction in work for institutions that wish to develop a broad set of scenarios.

- The threat events in the example scenario had multiple, plausible attack techniques. The detailed scenario identified only a minimal set of techniques for each threat event, to provide a concrete example of how the attack could be conducted. However, in a full-scale threat model analysis to assess enterprise defenses, threat analysts would need to consider the entire range of alternative techniques an attacker might employ.

Consequently, this effort has demonstrated that a more accurate gap analysis is supported by developing scenarios to test against the enterprise's existing security processes and defensive suite. Subsequent evaluation of the effectiveness of existing products may inform technology foraging to drive better choices for new technologies, or to assess the value of existing technologies in securing against threats. Finally, as new threat vectors and cyber attacks are identified, the ability to quickly understand the business process or technology changes needed to avoid potential impact to operations is enhanced.

This analysis, while it exhibited the value of such an approach, was only a small-scale demonstration using a notional enterprise as its subject. The application of such a threat model to a real-world enterprise would require much more extensive and thorough analysis, using multiple threat scenarios and considering all business areas, networks, and facilities.

5.2 Next Steps

Possible next steps to be undertaken include the following:

- Improve the threat model by incorporating risks from adoption of trending new technologies such as cloud. An architecture survey conducted by the NGCI program in 2016 (via interview of a sample of major financial institutions) showed no widespread adoption of external cloud shared-tenant environments for higher risk or availability sensitive applications. However, the use of virtual environments on hypervisor technology continues to grow, and the economics of shared clouds will remain a driver toward adoption.
- Use the methodology illustrated in this document to tailor the generic NGCI Apex threat model to individual institutions in line with their deployed set of processes, business technology, and security mitigation tools to provide a reusable residual risk framework to inform future decisions on changes to the security infrastructure.
- Leverage a repeatable residual risk framework to develop a consistent and repeatable set of assessment results to produce a more mature set of metrics that could be used to further understand the risk levels of components of the FSS. Existing sets of financial metrics, such as the Risk Assessment System (RAS) and CAMELS ratings[3] are common for FSS, but effective metrics in the technology and cyber arena remain an elusive goal.
- Develop sector-wide wargaming exercises that would serve as a follow-on to previous work such as the Hamilton series, to incorporate cyber risk metrics, tailored threat models, and residual risk frameworks based on deployed technology and process. Scenarios like the one illustrated in this document could be used within an interdependent

[3]A CAMELS rating is the result of a supervisory agency's assessment of a bank's condition, representing Capital adequacy, Asset quality, Management, Earnings, Liquidity, and Sensitivity to market risk (Lopez 1999).

system-of-systems context to produce variable effects based on risk components across institutions to validate the models and identify gaps in overall mitigation effectiveness.

Deployment of these maturation steps is needed to set in motion a common set of taxonomic components to measure, simulate, and derive understanding of the overall risk to the nation's money supply and ongoing economic stability due to potential cyber attack.

Appendix A Notional Financial Services Enterprise Detailed Cyber Defense Capabilities

Table 6 specifies the cyber defense capabilities of the notional financial services enterprise in greater detail. It maps the cyber defense capabilities described in Section 2.5 to the specific networks and business enclaves in which they are found. The color-coding represents the extent to which the defensive capability has been deployed in each of the enterprise's networks and business enclaves.

Table 6. Detailed Cyber Defense Capabilities

Legend

Y	= Deployed fully
N	= Not deployed, not planned
P	= Pilot program, experimental technology
I	= Incomplete deployment
T	= Targeted deployments only

Defensive Technology	Internet	Business-to-Business	Corporate WAN	Online Banking	Corporate Banking	Retail Banking	ATM Operations	Funds Transfer	Brokerage
Network									
Routers (ACLs)	Y	N	Y	Y	Y	Y	Y	N	N
Firewalls	Y	Y	N	N	N	N	Y	Y	Y
Web Application Firewalls	Y	N	N	N	Y	N	N	N	N
VPN concentrators	Y	N	N	N	N	N	N	N	N
Intrusion Detection and Prevention Systems (IDPS)	Y	T	T	N	N	N	N	Y	N
Sandboxes	I	N	N	N	N	N	N	N	N
Outbound web proxies	Y	N	N	N	N	N	N	N	N
Reverse proxies	Y	N	N	N	Y	N	N	N	N
Sinkholes	N	N	Y	Y	Y	Y	N	N	N
Netflow analytics	Y	N	Y	Y	Y	Y	N	N	N
Packet Recorders	I	N	N	N	N	N	N	N	N
DDoS prevention	Y	N	N	N	N	N	N	N	N
Compromise detection	I	N	N	N	N	N	N	N	N
Email Antivirus	Y	N	N	N	N	N	N	N	N
DNS Log Monitoring	Y	N	N	N	N	N	N	N	N

Defensive Technology	Internet	Business-to-Business	Corporate WAN	Online Banking	Corporate Banking	Retail Banking	ATM Operations	Funds Transfer	Brokerage
Data									
Data Loss Prevention	Y	N	N	N	N	N	N	N	N
Email Encryption	Y	N	N	Y	Y	Y	N	N	Y
Application Encryption	Y	Y	Y	Y	Y	Y	Y	Y	Y
Disk Encryption	N	N	T	T	T	T	Y	N	N
Database Activity Monitoring	N	N	N	N	T	N	N	N	N
Fraud Monitoring	Y	N	N	N	N	Y	N	N	N
Host									
Antivirus	Y	Y	Y	Y	Y	Y	Y	Y	Y
Host Based Intrusion Prevention (HIPS)	Y	N	N	N	T	N	N	Y	N
File integrity monitoring software	Y	Y	N	N	T	N	N	Y	N
Automated Patch Management and Distribution System	Y	Y	Y	Y	Y	Y	Y	Y	Y
Sandboxing applications	N	N	N	N	N	P	N	N	N
Application Whitelisting	N	N	N	N	P	N	N	N	N
Security Management									
SIEM	Y	I	I	I	I	I	N	N	I
Log Analytics	Y	I	I	I	I	I	N	N	I

Appendix B Risk Profile of Notional Financial Services Enterprise

Table 7 profiles the sources of potential cybersecurity risk within the notional financial services enterprise, based on the risk elements identified in the FFIEC CAT [FFIEC 2017]. It notes specifically in which networks and business enclaves each risk element is present.

Table 7. Notional Financial Services Enterprise Risk Profile

Legend

N	= Not deployed, not planned
Y	= Extensive deployment / use
S	= Select deployment / usage
P	= Pilot program, experimental technology
I	= Incomplete deployment

Category	Factor	Notional Enterprise High-Level Description	Internet	Business-to-Business	Corporate WAN	Corporate Banking	Retail Banking	Brokerage Application	Online Banking	Funds Transfer	ATM Operations	Brokerage Enclave
Technologies and Connection Types	Total number of Internet service provider (ISP) connections (including branch connections)	The five major data centers Some of the branches	Y	S	N	N	N	N	Y	N	N	Y
	Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None exist	N	N	N	N	N	N	N	N	N	N
	Wireless network access	Available universally at all branches and campuses	N	N	Y	N	N	N	N	N	N	Y
	Personal devices allowed to connect to the corporate network	BYOD is a formal program, used by business lines to reduce cost, allowed to connect directly to the wireless in branches and campuses	N	N	Y	N	N	N	N	N	N	Y
	Third parties, including number of organizations and number of individuals from vendors and subcontractors, with access to internal systems (e.g., virtual private network, modem, intranet, direct connection)	Connectivity for vendors to support their products deployed inside the WAN, typically provided via VPN in the Internet Access Facilities, a few cases are by B2B facilities	Y	Y	Y	Y	Y	Y	Y	N	Y	Y

Category	Factor	Notional Enterprise High-Level Description	Internet	Business-to-Business	Corporate WAN	Corporate Banking	Retail Banking	Brokerage Application	Online Banking	Funds Transfer	ATM Operations	Brokerage Enclave
	Wholesale customers with dedicated connections	B2B connectivity provided to institutional customers at major data centers via dedicated facilities	Y	Y	N	N	N	Y	Y	Y	Y	Y
	Internally hosted and developed or modified vendor applications supporting critical activities	Use of in-house development and modification of vendor products, supporting most lines of business, most reside in server farms, Internet Access, and B2B facilities.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Internally hosted, vendor-developed applications supporting critical activities	Used in server farms, Internet Access, and B2B facilities	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	User-developed technologies and user computing that support critical activities (includes Microsoft Excel spreadsheets and Access databases or other user-developed tools)	User-developed scripts, spreadsheets, and personal databases, most stored on desktops in branches and campuses	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	End-of-life (EOL) systems	End of life systems exist in some server farms	N	N	S	S	S	S	S	N	S	S
	Open Source Software (OSS)	Extensive use of OSS in all environments, both for home-grown applications and under the covers of vendor-purchased equipment	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Network devices (e.g., servers, routers, and firewalls; include physical and virtual)	Extensive network device footprint spanning major and minor data centers, campuses, branches, and other remote sites	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	Third-party service providers storing and/or processing information that support critical activities (Do not have access to internal systems, but the institution relies on their services)	Used in operational functions such as payroll, T&E, HR, and facilities maintenance, accessed on the Internet and by a few B2B connections	N	N	N	Y	Y	Y	Y	N	N	Y
	Cloud computing services hosted externally to support critical activities	Minimal cloud footprint, limited to deviations from policy	N	N	N	N	N	N	N	N	N	N

Category	Factor	Notional Enterprise High-Level Description	Internet	Business-to-Business	Corporate WAN	Corporate Banking	Retail Banking	Brokerage Application	Online Banking	Funds Transfer	ATM Operations	Brokerage Enclave
Delivery Channels	Online presence (customer)	Online presence is provided by Internet Access facilities and B2B links	Y	Y	N	N	N	N	Y	N	N	N
	Mobile presence	Mobile apps provided to customers that support each business line, all hosted in the Internet Access facilities	Y	N	N	N	N	N	Y	N	N	N
	Automated Teller Machines (ATM) (Operation)	ATM deployment is linked via the Campuses and Branches facilities	N	N	N	N	N	N	N	N	Y	Y
	Issue debit or credit cards	Issues both via branches and online requests	N	N	Y	Y	Y	N	N	N	N	N
	Prepaid cards	Issues via branches and online requests	N	N	Y	Y	Y	N	N	N	N	N
	Emerging payments technologies (e.g., digital wallets, mobile wallets)	Has a minimal payment technology footprint, but a pilot program is currently being spun up to evaluate the service	P	N	N	N	P	N	N	N	N	N
	Person-to-person payments (P2P)	Has a minimal payment technology footprint, but a pilot program is currently being spun up to evaluate the service	P	N	N	N	P	N	N	N	N	N
	Originating Automated Clearing House (ACH) payments	Origination on behalf of a commercial business customer, ACH routes credits to depository accounts at multiple banks with within the U.S. Most used for payroll, re-imbursement deposits	N	N	N	Y	Y	N	N	N	N	N
	Originating wholesale payments (e.g., Clearing House Interbank Payments System [CHIPS])	Larger value and non-critical time-based transactions. Clearing house net value exchange between member banks	N	N	N	Y	N	N	N	N	N	N
	Wire transfers	Any dollar value real-time money transfer between member banks. Platforms include FedWire and SWIFT	Y	Y	Y	Y	Y	N	Y	Y	N	N
	Merchant remote deposit capture (RDC)	Deposit documents are retained by the merchant and transaction detail is submitted remotely using digital data transfer	y	y	y	N	Y	N	Y	N	N	N

Category	Factor	Notional Enterprise High-Level Description	Internet	Business-to-Business	Corporate WAN	Corporate Banking	Retail Banking	Brokerage Application	Online Banking	Funds Transfer	ATM Operations	Brokerage Enclave
	Global remittances	Transfer of income to developing countries usually associated with migratory workers. Relatively low value individual transactions	N	N	N	N	y	N	N	N	N	N
	Treasury services and clients	Commercial banking support to business cash management and investments	Y	Y	Y	Y	N	N	N	N	N	N
	Trust services	Recurring payments and management of disbursement agreements and annuitized assets	N	N	N	N	N	N	N	N	N	N
	Act as a correspondent bank (Interbank transfers)	Smaller banks without a funds transfer or brokerage function hold depository accounts at larger banks to support any needed transactions	N	N	N	N	N	N	N	N	N	N
	Merchant acquirer (sponsor merchants or card processor activity into the payment system)	Depository support of businesses who accept credit cards. Usually includes point of sale transactions, clearing, and settlement services	N	Y	N	N	Y	N	Y	N	N	N
	Host IT services for other organizations (either through joint systems or administrative support)	Usually coupled with correspondent bank services. Provides account level IT processing for customers of small bank	N	Y	N	N	N	N	N	N	N	N
	Mergers and acquisitions (including divestitures and joint ventures)	Service to corporate customers on mergers or purchase of another company. Can provide legal, financial, stock, and management advice to transaction	N	N	N	N	N	N	N	N	N	N
	Direct employees (including information technology and cybersecurity contractors)	A considerable number of direct employees and contractors are used to develop, standardize, build, and maintain all IT assets in all facilities	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Category	Factor	Notional Enterprise High-Level Description	Internet	Business-to-Business	Corporate WAN	Corporate Banking	Retail Banking	Brokerage Application	Online Banking	Funds Transfer	ATM Operations	Brokerage Enclave
	Changes in IT and information security staffing	Because of the total number of employees and the scale of the operation, a regular stream of employees come and go. The enterprise has established procedures for departing employees and for onboarding.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Organizational Characteristics	Privileged access (Administrators-network, database, applications, systems, etc.)	In-house administrators have privileged access to assets in each facility. Administrators are grouped by functional area (server support, network support, etc.) not by business line.	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Appendix C Threat Events Mapped to Notional Financial Services Enterprise

Table 8 provides a comprehensive mapping of the events of the high-level threat model [Bodeau 2018] to the notional financial services enterprise. It notes specifically to which networks and business enclaves each threat event could apply.

Table 8. Mapping of High-Level Threat Events to Enterprise Networks and Business Functions

Legend

N	= Threat event does not apply
Y	= Threat event applies

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Internet	Business-to-Business	Corporate WAN	Online Banking	Corporate Banking	Retail Banking	ATM Operations	Funds Transfer	Brokerage Operations
Recon	Perform perimeter network reconnaissance/ scanning.	External network connection	Interception	Y	Y	N	N	N	N	N	N	Y
Recon	Perform network sniffing of exposed networks.	External network connection / Internal network (when CAL is applied recursively)	Interception	Y	Y	Y	Y	Y	Y	Y	Y	Y
Recon	Perform network sniffing of external networks (e.g., ISPs) to which organizational networks are connected.	External network connection	Interception	Y	Y	Y	Y	Y	Y	Y	Y	Y
Recon	Analyze network traffic based on network sniffing.	External network connection / Internal network (when CAL is applied recursively)	Interception	Y	Y	Y	Y	Y	Y	Y	Y	Y
Recon	Gather information using open source discovery of organizational information.	Publicly available information, social media interactions	Interception	Y	Y	Y	Y	Y	Y	Y	Y	Y

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Internet	Business-to-Business	Corporate WAN	Online Banking	Corporate Banking	Retail Banking	ATM Operations	Funds Transfer	Brokerage Operations
Recon	Perform reconnaissance and surveillance of targeted organizations.	Physical observation, social media interactions, in-person interactions, email, location tracking	Interception	Y	N	N	N	N	N	Y	N	Y
Recon	Perform malware-directed internal reconnaissance.	Maintenance environment, actions of privileged user, trusted or partner network connection	Interception	N	N	Y	Y	Y	Y	Y	Y	Y
Weaponize	Craft phishing attacks.	External network connection, email	(no immediate effects)	N	N	Y	Y	Y	Y	N	N	Y
Weaponize	Craft spear phishing attacks.	External network connection, email	(no immediate effects)	N	N	Y	Y	Y	Y	N	N	Y
Weaponize	Craft psychological manipulation attacks on key staff.	Social media interactions	(no immediate effects)	N	N	Y	Y	Y	Y	N	Y	Y
Weaponize	Craft attacks specifically based on deployed information technology environment.	External network connection, trusted or partner network connection	(no immediate effects)	Y	Y	Y	Y	Y	Y	Y	Y	Y
Weaponize	Create counterfeit/spoof web site.	External network connection	(no immediate effects)	Y	N	N	N	N	N	N	N	Y
Weaponize	Craft counterfeit certificates.	External network connection, trusted or partner network connection	(no immediate effects)	Y	N	N	N	N	N	N	N	Y

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Internet	Business-to-Business	Corporate WAN	Online Banking	Corporate Banking	Retail Banking	ATM Operations	Funds Transfer	Brokerage Operations
Weaponize	Create and operate false front organizations to inject malicious components into the supply chain.	Supply chain	(no immediate effects)	Y	Y	Y	Y	Y	Y	Y	Y	Y
Weaponize	Compromise systems in another organization to establish a presence in the supply chain.	Supply chain	(no immediate effects)	Y	Y	Y	Y	Y	Y	Y	Y	Y
Deliver	Establish or use a communications channel to the enterprise as a whole or to a targeted system.	External network connection, trusted or partner network connection	(no immediate effects)	Y	Y	N	N	N	N	Y	N	Y
Deliver	Deliver commands to a targeted system (e.g., login).	(no immediate effects)	Unauthorized use	Y	Y	N	N	N	N	Y	Y	Y
Deliver	Deliver known malware to internal organizational information systems (e.g., virus via email). (See CTF: Interact with intended victim)	External network connection, email	Corruption, Modification, or Insertion	Y	Y	Y	Y	Y	Y	Y	Y	Y
Deliver	Deliver modified malware to internal organizational information systems. (See CTF: Interact with intended victim)	Internal network, authorized actions of non-privileged user, authorized actions of privileged user, device port (e.g., removable media)	Corruption, Modification, or Insertion	Y	Y	Y	Y	Y	Y	Y	Y	Y

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Internet	Business-to-Business	Corporate WAN	Online Banking	Corporate Banking	Retail Banking	ATM Operations	Funds Transfer	Brokerage Operations
Deliver	Deliver targeted malware for control of internal systems and exfiltration of data.	Internal network, authorized actions of non-privileged user, authorized actions of privileged user, device port (e.g., removable media)	Corruption, Modification, or Insertion	Y	Y	Y	Y	Y	Y	Y	Y	Y
Deliver	Deliver malware by providing removable media.	Authorized actions of non-privileged user, authorized actions of privileged user, device port (e.g., removable media)	Corruption, Modification, or Insertion	N	N	Y	Y	Y	Y	Y	Y	Y
Deliver	Insert untargeted malware into downloadable software and/or into commercial information technology products.	Supply chain	Corruption, Modification, or Insertion	Y	Y	Y	Y	Y	Y	Y	Y	Y
Deliver	Insert targeted malware into organizational information systems and information system components.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Y	Y	Y	Y	Y	Y	Y	Y	Y
Deliver	Insert specialized malware into organizational information systems based on system configurations.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	Y	N	Y	Y	Y	Y	Y	Y	Y
Deliver	Insert counterfeit or tampered hardware into the supply chain.	Supply chain	Corruption, Modification, or Insertion	N	N	Y	Y	Y	Y	Y	N	N

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Internet	Business-to-Business	Corporate WAN	Online Banking	Corporate Banking	Retail Banking	ATM Operations	Funds Transfer	Brokerage Operations
Deliver	Insert tampered critical components into organizational systems.	Supply chain, maintenance environment	Corruption, Modification, or Insertion	N	N	Y	Y	Y	Y	Y	Y	Y
Deliver	Compromise information systems or devices used externally and reintroduced into the enterprise.	Mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	N	N	Y	Y	Y	Y	N	N	Y
Deliver / Exploit	Install general-purpose sniffers on organization-controlled information systems or networks.	Internal network, authorized actions of privileged user, device port (e.g., removable media)	Modification or Insertion	N	N	Y	Y	Y	Y	Y	N	Y
Deliver / Exploit	Install persistent and targeted sniffers on organizational information systems and networks.	Internal network, authorized actions of privileged user, device port (e.g., removable media)	Modification or Insertion	N	N	Y	Y	Y	Y	Y	N	Y
Deliver / Exploit	Insert malicious scanning devices (e.g., wireless sniffers) inside facilities.	Immediate physical proximity	Modification or Insertion	N	N	Y	Y	Y	Y	Y	N	Y
Exploit	Exploit physical access of authorized staff to gain access to organizational facilities.	Immediate physical proximity	(no immediate effects)	N	N	Y	Y	Y	Y	Y	Y	Y
Exploit	Exploit poorly configured or unauthorized information systems exposed to the Internet.	External network connection	Corruption, Modification, or Insertion	Y	N	N	N	N	N	N	N	N
Exploit	Exploit split tunneling on an end-user system to gain access to enterprise systems.	External network connection, end-user system	Exfiltration, Interception	Y	N	Y	Y	Y	Y	N	N	Y
Exploit	Obtain a legitimate account. (See CTF)	External network connection	(no immediate effects)	Y	Y	Y	Y	Y	Y	Y	Y	Y

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Internet	Business-to-Business	Corporate WAN	Online Banking	Corporate Banking	Retail Banking	ATM Operations	Funds Transfer	Brokerage Operations
Exploit	Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones). (See CTF: Establish illicit user access)	Mobile or transiently connected devices	Corruption, Interception	N	N	Y	Y	Y	Y	N	Y	Y
Exploit or Control	Exploit recently discovered vulnerabilities. (See ATT&CK: Lateral Movement)	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	Y	Y	Y	Y	Y	Y	Y	Y	Y
Control	Acquire privileges associated with a user account, process, service, or domain. (See ATT&CK: Credential Access)	Internal network, internal shared or infrastructure services	Unauthorized use	Y	Y	Y	Y	Y	Y	Y	Y	Y
Control	Modify or increase privileges associated with a user account, process, service, or domain. (See ATT&CK: Privilege Escalation)	Internal network, internal shared or infrastructure services	Modification or Insertion	Y	Y	Y	Y	Y	Y	N	Y	Y
Control	Perform internal reconnaissance. (See ATT&CK: Discovery; enabled by Install sniffer, Acquire privileges, or Modify privileges)	Internal network, internal shared or infrastructure services	Interception	N	N	Y	Y	Y	Y	N	N	N
Control	Exploit multi-tenancy in a cloud environment. (See ATT&CK: Lateral Movement; enabled by Obtain a legitimate account)	Internal shared or infrastructure services	Corruption, Interception	N	N	N	N	N	N	N	N	N

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Internet	Business-to-Business	Corporate WAN	Online Banking	Corporate Banking	Retail Banking	ATM Operations	Funds Transfer	Brokerage Operations
Control	Exploit vulnerabilities on internal organizational information systems. (See ATT&CK: Lateral Movement)	External network connection, trusted or partner network connection, internal network	Corruption, Modification, or Insertion, unauthorized use	N	N	Y	Y	Y	Y	Y	Y	Y
Control	Exploit vulnerabilities using zero-day attacks. (See ATT&CK: Lateral Movement)	External network connection, trusted or partner network connection, internal network, mobile or transiently connected devices	Corruption, Modification, or Insertion, unauthorized use	Y	Y	Y	Y	Y	Y	Y	Y	Y
Control or Execute	Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	External network connection, trusted or partner network connection, internal network	Degradation, Interruption, Corruption, Modification, or Insertion, unauthorized use	Y	Y	Y	Y	Y	Y	Y	Y	Y
Control	Exploit insecure or incomplete data deletion in multi-tenant environment.	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Exfiltration, Interception	N	N	N	N	N	N	N	N	N
Control	Violate isolation in multi-tenant environment.	Internal shared or infrastructure services	Degradation, Interruption, Exfiltration, Interception	N	N	N	N	N	N	N	N	N

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Internet	Business-to-Business	Corporate WAN	Online Banking	Corporate Banking	Retail Banking	ATM Operations	Funds Transfer	Brokerage Operations
Control	Establish command and control (C2) channels to malware or compromised components. (See ATT&CK: Command and Control)	External network connection, trusted or partner network connection, internal network, internal shared or infrastructure services	Corruption, Modification, or Insertion, unauthorized use, Exfiltration	Y	Y	N	N	N	N	N	Y	Y
Control	Employ anti-IDS measures. (See CTF; see ATT&CK: Defense Evasion)	Internal network, internal shared or infrastructure services	Modification, Insertion	Y	Y	Y	Y	Y	Y	Y	Y	Y
Control	Employ anti-forensics measures. (See CTF; see ATT&CK: Defense Evasion)	Internal network, internal shared or infrastructure services, internal system	Modification, Insertion	Y	Y	Y	Y	Y	Y	Y	Y	Y
Control	Compromise critical information systems via physical access.	Immediate physical proximity	Degradation, Interruption, Corruption, Modification, or Insertion, Unauthorized use	Y	Y	Y	Y	Y	Y	Y	Y	Y
Control	Compromise organizational information systems to facilitate exfiltration of data/information. (See CTF: Relocate and store data on victim's computer, information systems, networks, and/or data stores)	Maintenance environment, internal network, internal shared or infrastructure services, authorized action of privileged user, device port	Corruption, Modification, or Insertion, unauthorized use, Exfiltration, Exfiltration, Interception	Y	Y	Y	Y	Y	Y	Y	Y	Y

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Internet	Business-to-Business	Corporate WAN	Online Banking	Corporate Banking	Retail Banking	ATM Operations	Funds Transfer	Brokerage Operations
Control	Stage data for exfiltration. (See CTF: Relocate and store data on victim's computer, information system(s), network(s), and/or data stores; see ATT&CK: Collection)	Internal network, internal shared or infrastructure services, internal system	Insertion	Y	Y	Y	Y	Y	Y	Y	Y	Y
Control	Compromise information critical to mission / business functions.	Internal network, internal shared or infrastructure services, authorized action of non-privileged user, authorized action of privileged user, device port, data	Corruption, Modification, or Insertion	Y	Y	Y	Y	Y	Y	Y	Y	Y
Execute	Obtain sensitive information through network sniffing of external networks. (See ATT&CK: Collection)	External network connection, trusted or partner network connection	Interception	Y	Y	N	N	N	N	Y	Y	Y
Execute	Cause degradation or denial of attacker-selected services or capabilities. (See CTF: Deny access)	Internal network, internal shared or infrastructure services, authorized action of privileged user	Degradation, Interruption	Y	Y	Y	Y	Y	Y	Y	Y	Y

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Internet	Business-to-Business	Corporate WAN	Online Banking	Corporate Banking	Retail Banking	ATM Operations	Funds Transfer	Brokerage Operations
Execute	Cause deterioration/ destruction of critical information system components and functions. (See CTF: Destroy hardware / software / data)	Internal network, internal shared or infrastructure services, authorized action of privileged user	Degradation, Interruption	Y	Y	Y	Y	Y	Y	Y	Y	Y
Execute	Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement).	External network	Corruption, Modification, or Insertion	Y	N	N	N	N	N	N	N	N
Execute	Cause integrity loss by polluting or corrupting critical data. (See CTF: Alter data on the victim's system[s])	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Corruption, Modification	Y	Y	Y	Y	Y	Y	Y	Y	Y
Execute	Cause integrity loss by injecting false but believable data into organizational information systems.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, data	Insertion	Y	Y	Y	Y	Y	Y	Y	Y	Y

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Internet	Business-to-Business	Corporate WAN	Online Banking	Corporate Banking	Retail Banking	ATM Operations	Funds Transfer	Brokerage Operations
Execute	Reduce or deny availability by jamming communications.	External network, trusted or partner network connection, internal network	Degradation, Interruption	Y	Y	Y	Y	Y	Y	Y	N	Y
Execute	Cause disclosure of critical and/or sensitive information by authorized users.	Internal network, internal shared or infrastructure services, authorized action of privileged user, social engineering	Exfiltration, Interception	Y	Y	Y	Y	Y	Y	Y	Y	Y
Execute	Cause unauthorized disclosure and/or unavailability by spilling sensitive information.	Internal network, internal shared or infrastructure services, authorized action of privileged user, social engineering	Exfiltration, Interception	Y	Y	Y	Y	Y	Y	Y	Y	Y
Execute	Transmit sensitive information from the internal network to an external destination covertly. (See CTF: Exfiltrate data / information and ATT&CK: Exfiltration)	External network, trusted or partner network connection, internal network	Exfiltration	Y	Y	N	N	N	N	N	N	N
Execute	Inject crafted network traffic.	External network, trusted or partner network connection, internal network	Corruption, Modification, or Insertion	Y	Y	Y	Y	Y	Y	Y	Y	Y

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Internet	Business-to-Business	Corporate WAN	Online Banking	Corporate Banking	Retail Banking	ATM Operations	Funds Transfer	Brokerage Operations
Execute	Transmit messages to a targeted range of perimeter network addresses to deny service.	External network, trusted or partner network connection	Degradation, Interruption	Y	Y	N	N	N	N	N	N	Y
Execute	Download sensitive information to information systems or devices used externally and reintroduced into the enterprise.	Internal network	Exfiltration, Interception	N	N	Y	Y	Y	Y	N	N	Y
Execute	Obtain information by externally-located interception of wireless network traffic.	Internal network	Interception	N	N	Y	Y	Y	Y	N	N	N
Execute	Obtain unauthorized access.	Internal network, internal shared or infrastructure services, authorized action of privileged user, authorized action of non-privileged user, social engineering	Unauthorized use	Y	Y	Y	Y	Y	Y	Y	Y	Y
Execute	Obtain sensitive data/information from publicly accessible information systems.	External network	Exfiltration, Interception	Y	Y	N	N	N	N	Y	N	Y
Execute	Obtain information by opportunistically stealing or scavenging information systems/components.	Supply chain, maintenance environment	Exfiltration, Interception	Y	Y	Y	Y	Y	Y	Y	Y	Y

CAL Stage	Adversary Behavior or Threat Event	Attack Vector(s)	Cyber Effect(s)	Internet	Business-to-Business	Corporate WAN	Online Banking	Corporate Banking	Retail Banking	ATM Operations	Funds Transfer	Brokerage Operations
Maintain	Obfuscate adversary actions. (See ATT&CK: Defense Evasion)	Internal network, internal shared or infrastructure services, authorized action of privileged user	Corruption, Modification	Y	Y	Y	Y	Y	Y	Y	Y	Y

List of Acronyms

Acronym	Definition
ACH	Automated Clearing House
ACL	Access Control List
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
ATM	Automated Teller Machines
ATT&CK™	Adversary Tactics, Techniques, and Common Knowledge
B2B	Business-to-Business
BYOD	Bring Your Own Device
C2	Command and Control
CAMELS	Capital adequacy, Asset quality, Management, Earnings, Liquidity, and Sensitivity
CAPEC™	Common Attack Pattern Enumeration and Classification
CAL	Cyber Attack Lifecycle
CAT	Cyber Assessment Tool
CHIPS	Clearing House Interbank Payments System
CISO	Chief Information Security Officer
CTF	Cyber Threat Framework
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DNS	Domain Name System
DoS	Denial of Service
EOL	End-of-Life
FFIEC	Federal Financial Institutions Examination Council
FFRDC	Federally Funded Research and Development Center

Acronym	Definition
FSS	Financial Services Sector
Gbps	Gigabits Per Second
HIPS	Host-based Intrusion Prevention System
HSSEDI	Homeland Security Systems Engineering & Development Institute
ICS	Industrial Control System
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IOC	Indicator of Compromise
IP	Internet Protocol
IPS	Intrusion Protection Systems
IT	Information Technology
MPLS	Multiprotocol Label Switching
NFSE	Notional Financial Services Enterprise
NGCI	Next Generation Cyber Infrastructure
NGFW	Next Generation Firewall
NIST	National Institute of Standards and Technology
NYSE	New York Stock Exchange
OSS	Open Source Software
PBX	Private Branch Exchange
PC	Personal Computer
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
RAS	Risk Assessment System
RDC	Remote Deposit Capture
S&T	Science and Technology Directorate
SAN	Storage Area Network

Acronym	Definition
SIEM	Security Information and Event Management
SOC	Security Operations Center
SP	Special Publication
SSO	Single Sign-On
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TTP	Tactics, Techniques, and Procedures
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VoIP	Voice Over IP
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network

List of References

1. Bodeau, D., McCollum, C., and Fox, D. "Cyber Threat Modeling: Survey, Assessment, and Representative Framework," HSSEDI, The MITRE Corporation, March 2018.

2. Bodeau, D. and McCollum, C. 2018b. "Threat Model System-of-Systems Scenario," HSSEDI, The MITRE Corporation, May 2018.

3. Cloud Security Alliance. 2016. "The Treacherous 12 - Top Threats to Cloud Computing + Industry Insights," 2016. Available at https://cloudsecurityalliance.org/download/the-treacherous-twelve-cloud-computing-top-threats-in-2016/

4. FFIEC. 2017. "FFIEC Cybersecurity Assessment Tool," May 2017. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf

5. Fox, D., McCollum, C., Arnoth, E., and Mak, D. 2018. "Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context," HSSEDI, The MITRE Corporation, March 2018.

6. Fox, D., Arnoth, E., Skorupka, C., and McCollum, C. 2018b. "Enhanced Cyber Threat Model for Financial Services Sector (FSS) Institutions, Threat Model ATT&CK/CAPEC Version," Version 1.0, HSSEDI, The MITRE Corporation, March 15, 2018.

7. Hutchins, E.M., Cloppert, M.J., and Amin, R.M. 2010 "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proceeding of the 6th International Conference on Information Warfare and Security (ICIW 2011), Academic Conferences Ltd., 2011. Available at http://papers.rohanamin.com/wp-content/uploads/papers.rohanamin.com/2011/08iciw2011.pdf

8. Lopez, Jose. 1999. "Using CAMELS Ratings to Monitor Bank Conditions," Federal Reserve Bank of San Francisco Economic Letter, June 11, 1999. https://www.frbsf.org/economic-research/publications/economic-letter/1999/june/using-camels-ratings-to-monitor-bank-conditions/

9. The MITRE Corporation. 2015. "Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)," 2015. https://attack.mitre.org/wiki/Main_Page

10. The MITRE Corporation. 2016. "Common Attack Pattern Enumeration and Classification (CAPEC)," June 2016. https://capec.mitre.org

11. The MITRE Corporation. 2016b. "PRE-ATT&CK – Model to Improve Cyber Threat Detection Before Adversaries Compromise Your Network (PR 16-3852)" and "PRE-ATT&CK Briefing (PR 16-4128)," The MITRE Corporation, McLean, VA, November 30, 2016. https://attack.mitre.org/pre-attack/index.php/Main_Page

12. NIST. 2012. "Guide for Conducting Risk Assessments," NIST Special Publication 800-30, Revision 1, September 2012.

13. NIST. 2017. "Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1," January 10, 2017. https://www.nist.gov/sites/default/files/documents/draft-cybersecurity-framework-v1.11.pdf

14. NIST. 2017b. "The Cybersecurity Framework: Implementation Guidance for Federal Agencies," Draft NISTIR 8170, May 2017. http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf

15. ODNI. 2017. “The Cyber Threat Framework.” March 13, 2017. https://www.dni.gov/index.php/cyber-threat-framework, Overview: https://www.dni.gov/files/ODNI/documents/features/A_Common_Cyber_Threat_Framework_Overview.pdf, How to Use: https://www.dni.gov/files/ODNI/documents/features/A_Common_Cyber_Threat_Framework.pdf, Lexicon: https://www.dni.gov/files/ODNI/documents/features/Cyber_Threat_Framework_Lexicon.pdf, and Detailed Description: https://www.dni.gov/files/ODNI/documents/features/Threat_Framework_A_Foundation_for_Communication.pdf