HSSEDI
Homeland Security Systems Engineering & Development Institute

Prepared for:
Department of Homeland Security

System-of-Systems Threat Model

June 28, 2018

Authors:

Deborah J. Bodeau
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 18-1631 / DHS reference number 16-J-00184-07

This document is a product of the Homeland Security Systems Engineering and Development Institute (HSSEDI™).

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 explored the use of the general threat modeling framework developed under the NGCI Apex program for the Financial Services Sector (FSS) from a sector-level view or an institution-centric view, taking into consideration institutional links to partners, suppliers, and customers. This technical report describes system-of-systems views, identifies ways in which a system-of-systems threat scenario could be used, and demonstrates the potential utility of the general threat modeling framework by providing an initial system-of-systems scenario.

Key Words

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

This page intentionally left blank

Table of Contents

List of Figures

List of Tables

1 Introduction

A cyber threat model captures information about potential cyber threats against a system, an enterprise, a system of systems (SoS), a region, or a critical infrastructure (CI) sector.[1] A cyber threat model can serve as a basis for a variety of tasks at different scopes. For example, a system or sub-system can be analyzed against a set of threat events to identify capability gaps, and test cases can be developed using relevant threat events. At a broader scope, one or more systems of systems are involved. A comprehensive analysis of a system of systems against a set of threat events is often impractical; instead, analysis of systems of systems relies on the development and use of threat scenarios. A threat scenario tells the story of how a potential threat could materialize and result in harm or undesirable consequences. Figure 1 illustrates potential uses of threat scenarios at three scopes or scales involving systems of systems: the mission or business function, the enterprise, and the sector (or sub-sector) or region.

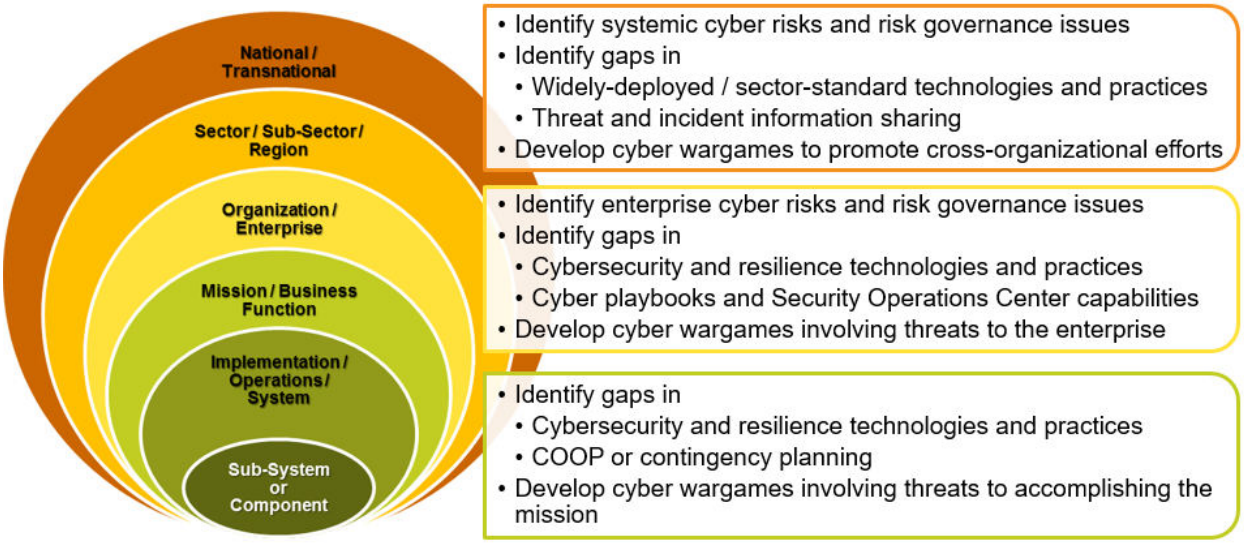

Figure 1. Uses of Cyber Threat Scenarios Involving Systems of Systems

1.1 Purpose

The Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) Next Generation Cyber Infrastructure (NGCI) Apex Program seeks to accelerate the adoption of cyber technologies proven to be effective for mitigating information technology (IT) security risk. As part of that effort, it is developing a cyber threat modeling framework applicable to the Financial Services Sector (FSS) that can provide a consistent frame of reference complementary to the threat models maintained internally by individual FSS institutions. The goals of the NGCI program are to 1) increase financial sector-wide situational understanding of evolving IT security risk and the technology associated with mitigating that risk; 2) improve the ability to understand and link compromises in the underlying cyber infrastructure to sub-sector operations; 3) enable greater information flows between sub-sectors as well as across the entire sector; and 4) enable

[1] A cyber threat consists of a threat source, a set of threat events caused by or actions taken by a threat source, and the expected cyber effects of those events or actions. See [Bodeau 2018] for more information.

FSS institutions to detect and neutralize adversaries more quickly and effectively than is currently possible. To achieve these goals, the NGCI Program requires threat modeling and development of threat scenarios beyond those at the level of individual institutions. This report explores how the cyber threat modeling framework, tailored and extended as necessary, can be used to develop such scenarios.

This report represents an initial exploration of system-of-systems cyber threat modeling. Directions for possible future work are also identified in this report.

1.2 Scope

In previous work, the Homeland Security Systems Engineering & Development Institute (HSSEDI) developed a threat framework and high-level threat model tailored to institutions in the financial services sector [Bodeau 2018]. HSSEDI then mapped the high level threat events in that model to implementation methods attackers might use to accomplish them, using community-consensus repositories of attack techniques to provide a more detailed extended threat model [Fox 2018b]. These models provide a means of examining an organization's cyber threat and risk from a microprudential perspective, i.e., cybersecurity threats directly facing an individual enterprise based on its technologies and services architecture and external interfaces. The use of the threat model for a concrete, though hypothetical, FSS institution is described in [Fox 2018c].

While such an individual model can be used to help identify local and third-party risks to an enterprise due to cyber threats, it does not provide a macroprudential perspective of cyber risks to sub-sector or sector functions involving the interaction of multiple institutions and utilities. Understanding these systemic cyber risks requires a threat model that recognizes the interconnection of functions within individual institutions into multi-institution systems of systems. This report provides first steps towards an enhanced threat model incorporating such a system-of-systems perspective.

1.3 Overview of This Document

Section 2 provides background on cyber threat modeling and issues related to threat modeling at the system-of-systems scale, and surveys prior work on threat scenarios at that scale for the FSS. Section 3 extends and tailors the cyber threat modeling framework defined in [Bodeau 2018] for systems of systems. Section 4 describes a general process for developing system-of-systems threat scenarios and provides a representative example of a system-of-systems threat scenario.

2 Background

This section provides a brief description of the previous threat model analysis HSSEDI conducted for the NGCI Apex program. It also provides a definition of a SoS and discusses issues related to threat modeling for SoS. Finally, it surveys prior work on threat scenarios developed for FSS SoS.

2.1 Threat Modeling Framework for FSS Institutions

In previous work [Bodeau 2018], HSSEDI conducted a survey of cyber threat models and threat modeling frameworks relevant to the goals and use cases of the NGCI Apex Program. This survey included a literature survey of 21 threat models and frameworks that are in broad use for managing cybersecurity, as well as interviews with executives at 11 large FSS institutions who are responsible for cyber threat modeling, risk assessment, and mitigation. Figure 2 illustrates the range of models and frameworks surveyed.

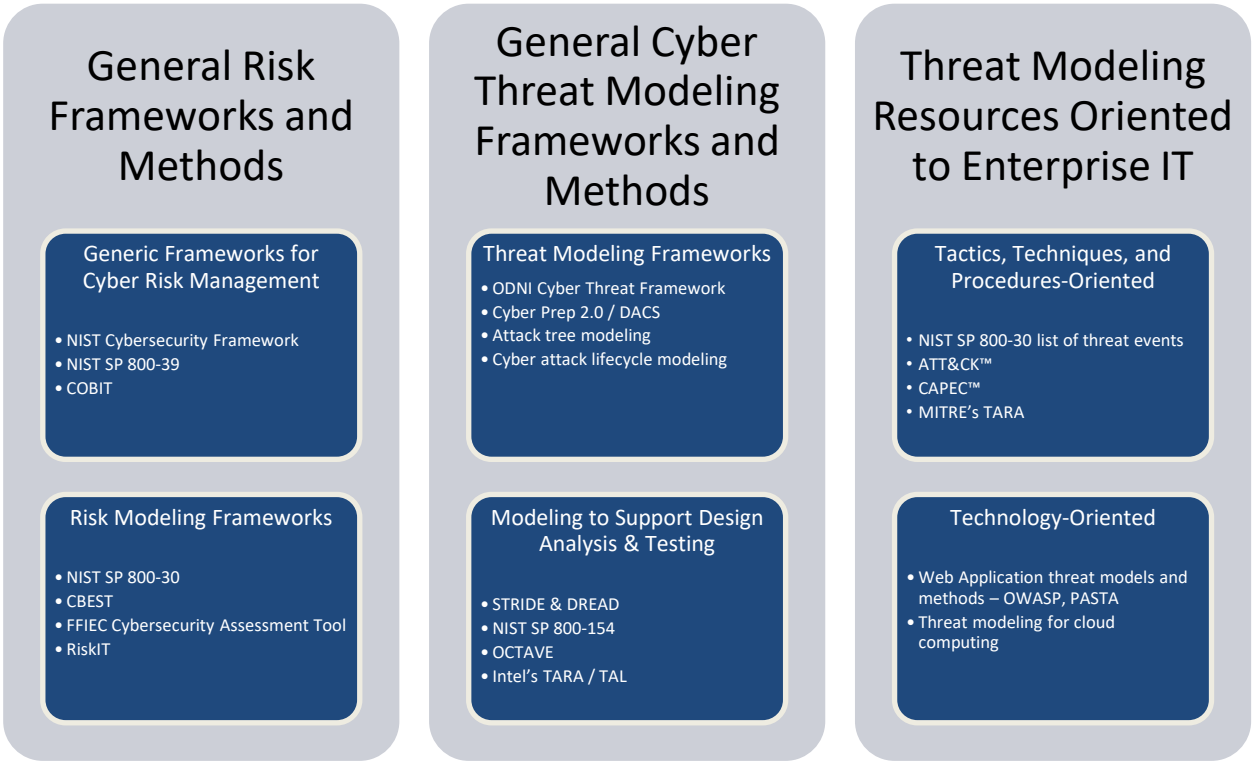

Figure 2. Cyber Threat Modeling Frameworks and Methods[2]

[2] Models surveyed include NIST SP 800-30 [NIST 2012], NIST SP 800-39 [NIST 2011], and the NIST Cybersecurity Framework [NIST 2014] [NIST 2018]; COBIT [ISACA 2012] and RiskIT [ISACA 2009]; CBEST [Bank of England 2016] and the FFIEC Cybersecurity Assessment Tool [FFIEC 2015]; the ODNI Cyber Threat Framework [ODNI]; Cyber Prep 2.0 [Bodeau 2016] and the DACS Framework [Bodeau 2014]; Microsoft's STRIDE and DREAD methodologies [Microsoft 2005]; SEI's OCTAVE / Allegro [Caralli 2007]; Intel's TARA and Threat Agent Library [Intel 2007]; ATT&CK [MITRE 2015], CAPEC [MITRE], and MITRE's Threat Assessment and Remediation Analysis (TARA) [Wynn 2011]; and the OWASP threat model [OWASP 2016]. For more information on these and others, see [Bodeau 2018].

HSSEDI defined criteria to assess the characteristics of the various threat models and their suitability for NGCI Apex. The analysis found that the models clustered into groups best suited for either strategic planning, engineering and acquisition, or operations. There was no one model, nor a cohesive suite of models, well suited for use at these three different levels of detail.

HSSEDI determined that there would be value in a coordinated suite of threat models to enable clear and consistent communication and to minimize gaps, both within and among FSS institutions or other enterprises. HSSEDI therefore laid out a framework within which such a coherent suite of threat models can be defined and populated, drawing upon extensive cyber attack information resources maintained and shared within the cybersecurity community. This is illustrated in Figure 3.

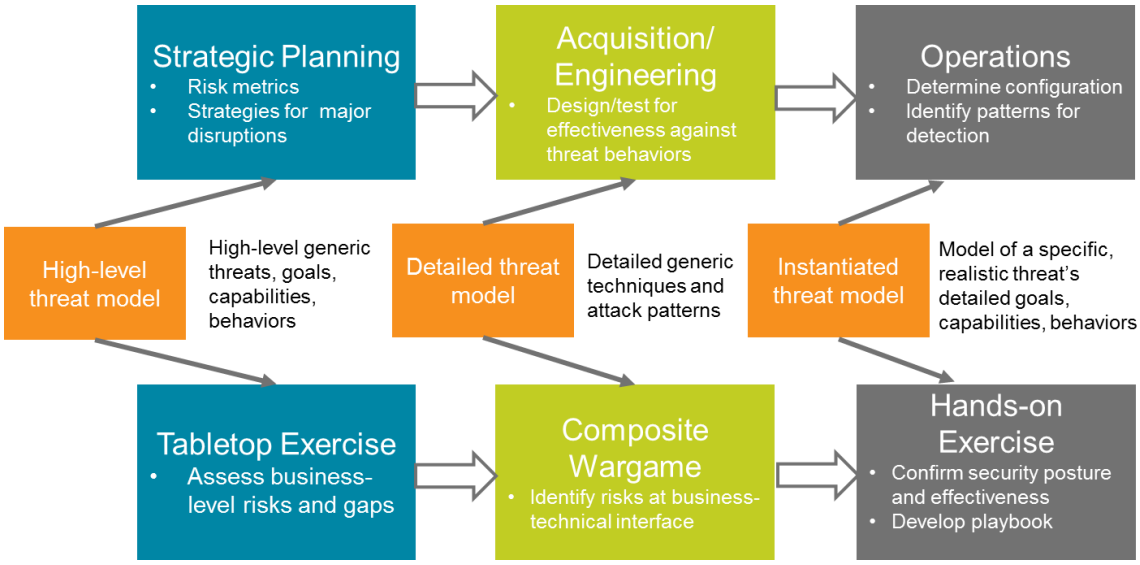

Figure 3. Three Levels of Cyber Threat Modeling

An initial, populated high-level threat model was provided as part of [Bodeau 2018]. This populated threat model corresponds to the strategic planning level of abstraction and serves as the top tier of a coordinated suite of threat models. An expanded threat model provided in [Fox 2018b] serves as the middle tier, corresponding to the acquisition/engineering level of abstraction. An example of how the expanded threat model can be used by a notional FSS institution is provided in [Fox 2018c].

The threat modeling framework developed for use by the NGCI Apex program is based on the National Institute of Standards and Technology (NIST) SP 800-30R1 framework [NIST 2012] and consists of:

- A set of general threat modeling constructs, as illustrated in Figure 4. (Constructs and relationships in dotted lines are included to indicate linkages to risk modeling; these constructs are used in risk assessment.) In each case, the verb should be modified with "one or more;" for example, a threat scenario has one or more consequences. These general threat modeling constructs are independent of the type of threat source, which can be adversarial or non-adversarial; non-adversarial types to information systems include human error, structural failure, and natural disaster. Additional constructs related to

adversarial threats are illustrated in Figure 5. Representative values are identified for selected attributes of an adversarial threat source: goal or motivation, intended cyber effect, timeframe, level of persistence, and degree of concern for stealth. The attributes illustrated in Figure 5 relate to an adversary's intent; the general framework also identifies additional attributes related to targeting (scope or scale of intended effects, types of assets targeted) and capabilities (resources, methods, and attack vectors).

- An initial set of adversary behaviors and adversary-related threat events. These are drawn primarily from NIST SP 800-30R1 [NIST 2012] but have been tailored for adversaries with characteristics identified as representative of attackers targeting FSS institutions.
- A small set of highly general threat scenarios that can serve as a starting point for development of more detailed, but still institution-independent, scenarios.

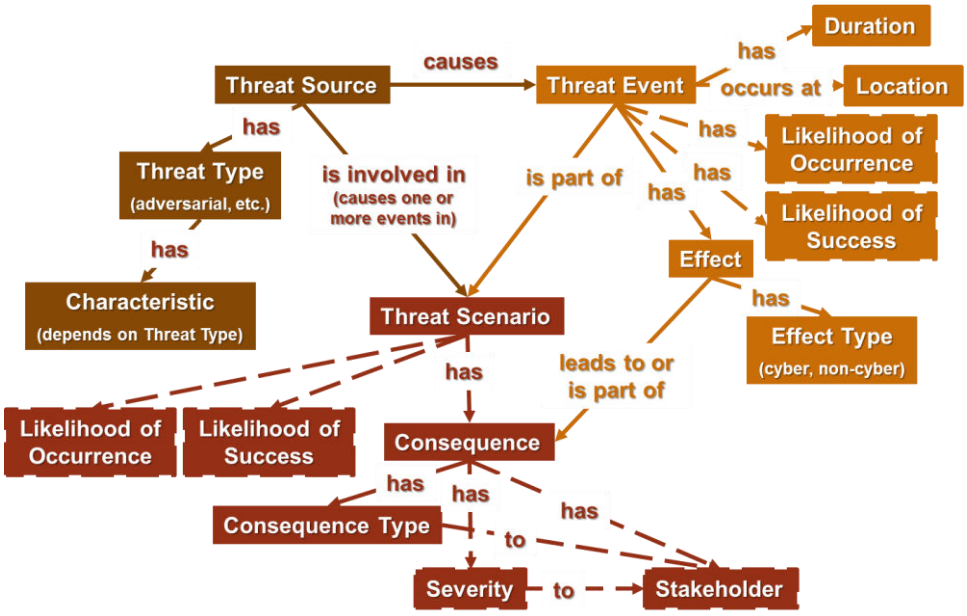

Figure 4. Key Constructs in Cyber Threat Modeling (Details for Adversarial Threats Not Shown)

The cyber threat modeling framework described above is oriented to a single institution, its missions or business functions, and its systems. Several questions arise when considering cyber threat modeling at a scope beyond a single institution:

- Does this set of threat modeling constructs suffice? Should some constructs be eliminated, should new constructs be added, and should the sets of representative values be modified?
- Does it make sense to include a catalog, taxonomy, or set of representative adversary behaviors and threat events?
- Can a set of representative threat scenarios, or sub-scenarios, be defined for general use?

Answers to these questions depend on an understanding of the modeling challenges for systems of systems, as well as the possible uses of system-of-systems cyber threat modeling.

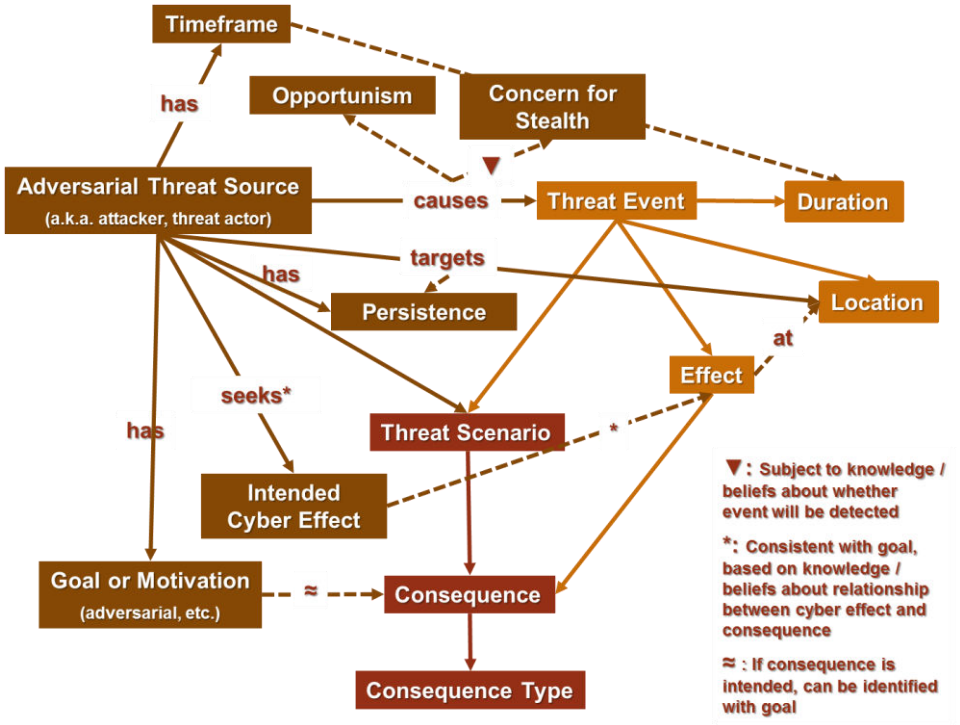

Figure 5. Key Constructs for Adversarial Threats

2.2 Systems of Systems

Multiple definitions of the term "system of systems" have been offered. For purposes of this report, a system of systems is a system whose elements are themselves systems [NIST 2016]; these are referred to as *constituent systems*.

> "*A system of systems (SoS) brings together a set of systems for a task that none of the systems can accomplish on its own. Each constituent system keeps its own management, goals, and resources while coordinating within the SoS and adapting to meet SoS goals.*" [ISO 2015], Annex G

Each constituent system in a system of systems has an owner and/or operator organization.[3] In the FSS, these organizations are typically financial institutions, infrastructure providers, or quasi-independent subsidiaries of financial institutions. In this report, the phrase "participant institution" is used to refer to the owner or operator of a constituent system in a system of systems.

As described in the subsections below, the FSS can be viewed as an ecosystem of sub-sectors, where each sub-sector is identified with a mission or set of business functions which spans multiple institutions and is supported by a system of systems of a well-defined type. Several general challenges to modeling cyber threats in a system-of-systems context can be identified.

[3] The concept of owners and operators is central to critical infrastructure protection. See [Bodeau 2013].

2.2.1 Systems of Systems in the FSS

As described in [HSSEDI 2018], the FSS is an ecosystem with intrinsic interdependencies. Its sector and sub-sector functions occur emergently through the efforts of multiple enterprises collaboratively performing their individual roles, and their success can be affected through cyber threats to individual entities.

The functions of the financial services sector can be grouped into the following sub-sectors [FSSCC 2015] [HSSEDI 2018]:

- Deposit, consumer credit, and payment systems;
- Credit and liquidity products;
- Investment products; and
- Risk transfer products, including insurance.

Systems of systems are evident in each of these sub-sectors. For instance, in the deposit, consumer credit, and payment systems sector, collaborative interaction of multiple institutions is involved in accomplishing wire transfers, check processing, and credit card processing. Regulators have recognized the criticality of some of these interdependencies by designating certain institutions and market utilities as systemically important, and imposing elevated requirements on their operations and health to ensure that functions in which they play a role are not unnecessarily put at risk.

2.2.2 Types of Systems of Systems

Four types of systems of systems have been defined ([Maier 1998] and [Defense Acquisition University 2013], quoted in [Bodeau 2013]):[4]

- **Virtual SoS** – A virtual SoS lacks a central management authority and a centrally agreed upon purpose for the system of systems. Large-scale behavior emerges, and although it may be desirable, this type of SoS must rely upon relatively invisible mechanisms to maintain it. The set of critical infrastructure systems in a region – including telecommunications, energy, and FSS institutional systems – can be viewed as a virtual SoS, as can the financial services sector as a whole.
- **Collaborative SoS** – In a collaborative SoS, the constituent systems interact more or less voluntarily to fulfill agreed upon central purposes. The central players collectively decide how to provide or deny service, thereby providing some means of enforcing and maintaining standards. Collaborative SoS can be identified with FSS sub-sectors or sets of FSS institutions relying on a given infrastructure (e.g., the Society for Worldwide Interbank Financial Telecommunication [SWIFT] or the United States [U.S.] Federal Reserve funds transfer system). Thus, the National Market System (NMS) is an example of a collaborative SoS.
- **Acknowledged SoS** – An acknowledged SoS has recognized objectives, a designated manager, and resources for the SoS; however, the constituent systems retain their independent ownership, objectives, funding, and development and sustainment

[4] These are also referred to as ecosystem, coalition, collaborative, and directed [Cliff 2011].

approaches. An enterprise network for a FSS institution that supports a variety of separate missions (e.g., funds transfer, brokerage, online banking) is an acknowledged SoS.

- **Directed SoS** – A directed SoS is one in which the integrated SoS is built and managed to fulfill specific purposes. It is centrally managed during long-term operation to continue to fulfill those purposes as well as any new ones the system owners might wish to address. The constituent systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose. A data center can be an example of a directed SoS.

2.2.3 Modeling Challenges for Systems of Systems

This report focuses on collaborative and acknowledged systems of systems, but also includes virtual SoS. These three classes of SoS present several challenges for threat modeling efforts, including:

- **Risk governance**. The participating institutions can frame risk differently, due in part to different legal or regulatory regimes. Differences in risk framing include differences in assumptions about the goals and capabilities of cyber adversaries, as well as the types of mitigations which may be applied under different circumstances.
- **Visibility**. The participating institutions may seek to limit the types and quality of information they share about the cybersecurity technologies and practices they use, the vulnerabilities they are currently unable to mitigate, and the threats which they have observed.
- **Level of abstraction**. For large-scale systems of systems, the constituent systems are often themselves systems of systems. For purposes of developing a threat scenario, trade-offs are needed between using a single level of abstraction (which can result in some threat events being so high-level as to appear vacuous) or allowing multiple levels of specificity when representing the set of activities in the scenario (which can result in confusion).
- **Complexity**. Collaborative and virtual systems of systems are generally complex; constituent systems were implemented using different architectures, at different times, for multiple purposes. Some dependencies among constituent systems in a system of systems are known or knowable, using analytic methods such as mission thread analysis [Woody 2014] or crown jewels analysis [MITRE 2016]. Others, however, are revealed only when a constituent system malfunctions or fails.
- **External dependencies**. A system of systems identified with a mission or business function does not exist solely in the context of executing the shared mission or performing different tasks in the common sub-sector function. It also exists in the context of dependence by constituent systems and participating institutions on supply chains, other critical infrastructures (notably electrical power, telecommunications, and transportation), and organizations engaged in cyber defense, incident response, and oversight; these can include information sharing entities such as the Financial Sector Information Sharing and Analysis Center (FS-ISAC), law enforcement agencies, and regulatory agencies. The scope of a cyber threat modeling framework or a cyber threat scenario must be bounded, with assumptions about external dependencies clearly stated.

2.3 Prior Work on System-of-Systems Cyber Threat Modeling

Prior work that includes system-of-systems cyber threat modeling includes:

- Multi-institution cyber exercises.
- Systemic risk analysis, including modeling and simulation (M&S) of cyber threat scenarios.
- Frameworks to support analysis of reported incidents and events at the sector or regional level.
- Systems engineering for system-of-systems security and cyber resiliency.

Efforts in these areas have been made for the FSS; for other critical infrastructure sectors or classes of systems, missions, or business functions; or for regions. The following subsections focus on the FSS.

2.3.1 Cyber Exercises

As discussed in [Fox 2018], a variety of threat scenarios have been developed and used for cyber exercises for the FSS, at the sub-sector level. These include scenarios developed for the Hamilton and Quantum Dawn series of exercises.

In the Hamilton Alliance series of tabletop exercises, "scenarios examined impacts to different segments of the financial sector, including impacts to equities markets, large, regional, and medium-sized depository institutions, payments systems and liquidity, and futures exchanges" [FSSCC 2017]. While the specific scenarios have not been widely shared,[5] they are reported to include a destructive malware attack as well as a major disaster event [Center for Homeland & Cyber Security 2017]. The focus in these scenarios is on the response of the participant institutions to the injected disruption; adversaries are not profiled.

In the Quantum Dawn series, a combination of tabletop and M&S activities used scenarios to simulate a series of attacks on individual institutions and on sector-wide functions. In Quantum Dawn 4, the simulated attack affected equity and fixed income futures transactions impacting the associated cash markets and the payments processes for foreign exchange [SIFMA 2017]. In Quantum Dawn 3, the sector-wide function was settlement [Deloitte 2015]; malware was introduced into clearing systems, causing major settlement failures. In Quantum Dawn 2, the focus was on procedures for closing the equity markets. Examples of attack scenarios targeted at individual institutions include a domain name system (DNS) attack, a distributed denial of service (DDoS) attack, an insider breach of personally identifiable information (PII), and lost availability due to an insider compromise of an exchange router [Deloitte 2015]. The focus in these scenarios is on the response of the participant institutions to the injected disruption; adversaries are not profiled.

2.3.2 Systemic Risk Analysis

In finance, the phrase "systemic risk,"

[5] The after-action reports of the Hamilton exercises are shared on a need-to-know basis.

> "generally refers to the risk of a disruption to the flow of financial services that is (i) caused by an impairment of all or parts of the financial system and (ii) has the potential to have serious negative consequences on the real economy. Systemic risk arises when the failure of a single entity or cluster of entities can cause a cascading failure, due to the size and the interconnectedness of institutions, which could potentially bankrupt or bring down the entire financial system."[6]

Network representations of FSS functions are used to analyze systemic risk [Allen 2009] [Battiston 2010], comparing the susceptibility of different network topologies to cascading failures or contagion [Roukny 2013]. Network analysis of systemic risk can also consider herding models as well as cascades and contagion [Lorenz 2009]. Two topologies are identified as paradigmatic [Bardoscia 2017]: a "butterfly" (or a "bow-tie") network and a core-periphery network. Network analyses for systemic risk analysis of the FSS focus on institutions rather than on constituent systems in a system of systems.

Systemic cyber risk is a topic of increasing interest for the FSS:

> "Systemic cyber risk is the risk that a cyber event (attack(s) or other adverse event(s)) at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security or national security." [World Economic Forum 2016]

The question of whether, or the extent to which, systemic cyber risk contributes to systemic risk is the subject of debate [Danielsson 2016]. However, incidents such as the MongoDB ransomware attacks [ENISA 2017], the Dyn DDoS attack [Lewis 2017], and the Society for Worldwide Interbank Financial Telecommunication (SWIFT) banking attacks [Schwartz 2016] are cited as examples of how systemic cyber risks can materialize [AIG 2017].

System-of-systems threat modeling is part of the analysis of systemic cyber risks for critical infrastructures. Systemic cyber risk arises from interdependencies, whether known or undiscovered. Known interdependencies among constituent systems can be represented using Functional Network Dependency Analysis (FNDA) [Garvey 2012], to support the modeling and simulation of cyber attacks in a system of systems [Guariniello 2014].

2.3.3 Frameworks to Support Analysis

Analysis of reported incidents and events (and, to a lesser extent, of prospective attacks) at the sector or regional level differs from analysis at the system or organizational level in that it looks for patterns or trends, rather than for indicators (e.g., artifacts) which can be used to inform activities in a Security Operations Center (SOC). Sector-scale threat analysis makes use of frameworks for characterizing cyber adversaries at the system-of-systems level, or for characterizing threat scenarios to a sector or sub-sector. The results of sector-scale threat analysis are typically published by sector organizations, or by teams at security service providers.

Frameworks for characterizing cyber adversaries are integral to various reports on systemic risk. For the financial services sector, these include a 2014 report by the Depository Trust & Clearing

[6] See http://www.systemic-risk-hub.org/.

Corporation (DTCC) [DTCC 2014], which adopts the CHEW (criminals, hacktivists, espionage, war) taxonomy of threat actors. A threat actor typology to support cyber threat analysis by the National Cyber Security Centre (NCSC) of the Netherlands, with strong emphasis on threats to the financial sector, characterizes eleven types of adversaries in terms of targets, expertise, resources, organization, and motivation [de Bruijne 2017].

A report from the Institute of International Finance [Boer 2017] identifies four classes of threat scenarios to the financial system: an attack on payment systems, attacks on integrity of data, failure of a wider infrastructure, and loss of confidence "because of a few very significant cyber-attacks or many very frequent successful smaller attacks on financial institutions or on financial markets infrastructures."

A 2018 report by DTCC and Oliver Wyman [Gray 2018] identifies five classes of attack scenarios which can have systemic consequences for the FSS: deletion of critical data (e.g., via ransomware), manipulation of critical data, disruption of critical industry-wide services, fraudulent transactions leveraging a critical infrastructure, and theft of critical non-public information.

A general framework for defining cybersecurity simulation scenarios identifies two broad groups of scenario elements: cyber systems (including data and network infrastructures) and actors (attackers, users, and system security personnel) [Kavak 2016].

Analysis of security trends in the FSS include such threat modeling constructs as:

- Classes of incidents (e.g., data breaches, DDoS, and malware attacks, including ransomware) and methods of attack (e.g., using the Common Attack Pattern Enumeration and Classification™ [CAPEC™] mechanisms of attack[7]) [Alvarez 2017].
- Adversary tactics, techniques, and procedures (TTPs) observed in attacks against FSS institutions (e.g., source code merging, sandbox evasion, remote desktop access, diversion, web injects, redirection, session hijacking, fileless load points, overlay forms, AtomBombing injection, and social engineering attacks) [Wueest 2017].
- Shifts in threat scenarios from consumer financial fraud to scenarios (i) targeting business customers, e.g., via business email compromise (BEC), (ii) involving malware targeting mobile banking, or (iii) targeting banks' core networks (e.g., to attack automated teller machine [ATM] networks), and shifts in adversary characteristics to (i) more sophisticated, better organized adversary groups, (ii) nation state hackers targeting banks, and (iii) easier access to nation state level capabilities by criminal groups [Carter 2017].

2.3.4 Systems Engineering

Systems engineering for systems of systems applies primarily to directed and acknowledged systems of systems, but can also be used to identify technical standards and good practices for collaborative (and to a lesser extent) virtual SoS. While these uses are not currently the focus of the NGCI Apex Program, some resources related to SoS modeling may be relevant. These include the framework for SoS security engineering [Dahmann 2015], which highlights the

[7] See http://capec.mitre.org.

importance of criticality analysis; the hybrid threat modeling method (hTMM) developed by the Software Engineering Institute (SEI) [Mead 2018], which combines the Security Cards approach to characterizing adversaries[8], the Persona non Grata (PnG) representation of typical users behaving badly, and Microsoft's STRIDE (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege) [Microsoft 2005].

[8] See https://securitycards.cs.washington.edu/.

3 System-of-Systems Threat Modeling Framework

This section describes a general framework for system-of-systems cyber threat modeling. This framework extends the previously defined framework for FSS institutions [Bodeau 2018] by tailoring existing threat modeling constructs and defining additional constructs.

3.1 Tailor Existing Threat Modeling Constructs

The adversary characteristics related to capabilities and intent identified in [Bodeau 2018] carry over to the system-of-systems environment largely unchanged. Attacker goals can be broadly characterized as direct financial gain (theft, extortion), indirect financial gain or other advantage (data breach), and service or sector disruption. As noted in a report by the Office of Financial Research (OFR), these goals can be achieved by causing incidents that disrupt the operations of a critical FSS institution, reduce overall confidence in the financial system, or damage the integrity of key data [OFR 2017].

In addition, characteristics related to targeting are tailored to reflect the broader scale on which an adversary in a system-of-systems threat scenario operates. Rather than focus on specific assets or asset types, adversary targeting in system-of-systems threat modeling focuses on sub-sectors or specific business functions. (See Section 2.2.1.) For systems of systems, three aspects of scope can be considered:

- **Technical scope**: how specifically or broadly are technologies (or specific systems) targeted. A narrow scope can focus on a single operating system (OS), database management system (DBMS), or router, or even on a specific version. An adversary with a broad technical scope may develop or acquire an arsenal of attack tools.
- **Functional scope**: how narrowly or broadly a business function, sub-sector, or sector is targeted. An adversary taking a narrow functional scope can be expected to develop or acquire intelligence about target systems and institutions involved in that function, to identify weak links in transaction chains. An adversary with a broad functional scope can be expected to focus on linchpin systems or services (e.g., DNS, as in the Dyn attack).
- **Institutional scope**: whether the adversary's targeting focuses on a single institution or on a family of institutions. An adversary taking a narrow institutional scope can be expected to develop or acquire intelligence about the institution's systems, personnel, and supply chain. An adversary with a broad institutional scope can be expected to look for technologies, services, or infrastructures commonly used by those institutions.

In Table 1, the intended scope refers to the basis on which an adversary targets systems (institutional, technical, or functional), either narrowly or broadly. The effective scope refers to the set of institutions or systems which could be affected by an attack with that intended scope. An institutionally narrow scope falls into the domain of enterprise threat modeling, rather than system-of-systems threat modeling, unless the targeted institution plays a central role in a sector function.

Table 1. Scope of Adversary Targeting

Focus	Intended Scope (Narrow (N), Broad (B))			Effective Scope
	Institutional	Technical	Functional	
Target a single institution	N	(any)	(any)	Institutional: Can affect the reputation or stability of the institution System-of-systems: Depends on the role of the institution in the system of systems – ranges from no effect (system-of-systems functions route around the damaged institution) to significant effect on the sector function and its constituent systems if the institution provides a unique capability to the sector function Broadly institutional: Depends on the role of the institution – can affect the set of institutions partnered with or dependent on the target institution for that function
Target a specific technology independent of its users	B	N	B	System-of-systems: Can affect a system of systems in which that technology is commonly used Broadly institutional: Can affect many or all institutions dependent on that technology
Target all systems that support a given sector function and that rely on a specific technology (e.g., a single OS)	B	N	N	System-of-systems: Can affect that sector function and its constituent systems (degree of consequence depends on degree of diversity, other cyber resiliency techniques) Broadly institutional: Can affect the set of institutions involved in that sector function
Target systems at multiple institutions supporting a given sector function	B	B	N	System-of-systems: Can affect that sector function and its constituent systems (degree of consequence depends on degree of diversity, other cyber resiliency techniques) Broadly institutional: Can affect the set of institutions involved in that sector function Systemic: Can affect public confidence in the targeted function; can affect the sector or the financial system as a whole

Focus	Intended Scope (Narrow (N), Broad (B))			Effective Scope
	Institutional	Technical	Functional	
Target systems and institutions across a region, a sector, or multiple sectors	B	B	B	System-of-systems: Can affect that sector function and its constituent systems (degree of consequence depends on degree of diversity, other cyber resiliency techniques) Broadly institutional: Can affect the set of institutions involved in that sector function Broadly systemic: Can affect public confidence in the targeted function; can affect the sector or the financial system as a whole; can affect national security

The set of threat events and adversary behaviors in Table 15 of [Bodeau 2018] apply to an institution and the systems it owns or operates. For system-of-systems threat modeling, a set of less granular threat events can be used to reflect the fact that visibility into constituent systems is limited. The descriptions of these threat events reflect the state and/or behavior of the constituent systems. Table 2 identifies an initial set of high-level threat events for use in defining system-of-systems threat scenarios. With the exception of the first event, the events in Table 2 reflect actions an adversary might take to orchestrate the use of compromised resources, in order to achieve systemic effects. Note that Table 2 is illustrative rather than exhaustive; a survey of historical attacks could yield additional high-level threat events.

Table 2. Initial Set of High-Level Threat Events

High-Level Threat Event in an Attack on a System of Systems
Gather intelligence about the system of systems, e.g., its structure, decision model, and defense model
Gather intelligence about constituent systems, e.g., commonly used technologies, external dependencies, supply chains
Gather intelligence about participant institutions, e.g., preparedness strategies
Compromise (install malware and maintain a presence on) a constituent system
Compromise a supporting system (e.g., a development, maintenance, or configuration management system)
Compromise an unrelated system potentially or actually connected to (i.e., sharing the same network with) a constituent system (as in the attack on the Target point-of-sale system)
Use a compromised system to observe the operational status of other constituent systems (e.g., latency in response to ping)
Use a compromised system to observe the security posture of other constituent systems (e.g., responses to attempted transactions with false credentials)
Use a compromised system to propagate malware to other constituent systems
Use a compromised system to launch denial of service (DoS) attacks on other constituent systems

High-Level Threat Event in an Attack on a System of Systems
Use a compromised system to send fabricated or modified business data to other constituent systems
Use a compromised system to inject fabricated transactions
Use a compromised system as a command and control (C2) node, i.e., to direct the behavior of malware on other constituent systems
Maintain situational awareness of the system of systems (in particular, watch for evidence of detection)
Launch a DoS or DDoS attack on a common infrastructure element of the system of systems (e.g., a network)
Launch a DoS or DDoS attack on a shared service element of the system of systems (e.g., an identity or credential management service)
Deny use of a constituent system, to degrade or deny service of the system of systems
Delete critical data on a compromised system in order to degrade or deny completion of transactions in the system of systems

3.2 Define Additional Threat Modeling Constructs

Several additional factors influence the types of attack activities an adversary might perform, and thus the definition of a threat scenario from threat events and adversary characteristics. These include additional characteristics of adversary targeting, as well as characteristics of the system of systems.

3.2.1 Additional Characteristics for Targeting

Two additional aspects of targeting are identified for system-of-systems attacks: control strategy (how actively the adversary engages in attack activities) and characteristics of potentially targeted institutions.

3.2.1.1 Adversary Control Strategy

In an attack on a system of systems, an adversary can propagate and direct malware on multiple systems in several different ways:

- **Closely directed**. The adversary directs the behavior of installed malware on an ongoing basis, monitoring the status of malware and coordinating activities on different systems and deciding whether and when to propagate malware to additional systems. The adversary must construct and maintain a C2 infrastructure and maintain ongoing situational awareness of compromised resources.
- **Loosely directed**. The adversary propagates malware and directs activities based on reports from successfully installed malware. The adversary must construct and maintain a C2 infrastructure, but does not need ongoing situational awareness or ongoing engagement with installed malware.
- **Contagion-based**. The adversary releases malware (e.g., via a watering hole) and directs activities from successfully installed malware after that malware reports back. This strategy is common for worms and viruses propagating ransomware. The attack is

ultimately against individual systems and organizations, but takes advantage of how individual systems participate in a system of systems to propagate.

- **Autonomous**. As in a contagion-based strategy, the adversary releases malware. However, the adversary does not receive reports from successfully installed malware or direct the released malware in any way. The attack is against any system which can be successfully infected, and takes the form of a disruption or denial of service triggered by date and time (i.e., a time bomb) or by other circumstances coded into the malware.

The adversary's control strategy is aligned with its intelligence gathering strategy. Two dimensions can be identified: focus and engagement. Intelligence gathering can be passive or active [NSA 2018]. Passive intelligence gathering involves open source searches, the purchase of the results of activities by others via black and gray markets [Ablon 2014], and non-cyber methods (e.g., dumpster diving or physical observation) [NSA 2018]. Active intelligence gathering involves interaction with target institutions or systems (e.g., via port scanning). Intelligence gathering can be narrowly focused on a well-defined set of target institutions or functions, or can be unfocused. For example, an adversary can perform an active, unfocused scan of the Internet [Infosec Institute 2017].

3.2.1.2 Institutional Targeting

An adversary with sufficient resources and motivation to attack a system of systems, rather than simply an individual institution, can be expected to perform intelligence gathering, analysis, and planning that takes into consideration the defensive strategy and capabilities of the institutional owners or operators of constituent systems. Such an adversary can target institutions with a lower level of cyber preparedness – the weak links in the system of systems chain.

As illustrated in Figure 6, attributes of an institution's strategy for preparedness against cyber threats can be captured using Cyber Prep levels [Bodeau 2016], or levels of Cyber Prep aspects in the areas of governance, operations, and architecture / engineering. This information can be represented by an overall level, individual levels for the three areas, or by using the Cyber Prep profiling questionnaire [Sheingold 2017] to obtain individual levels for each aspect.

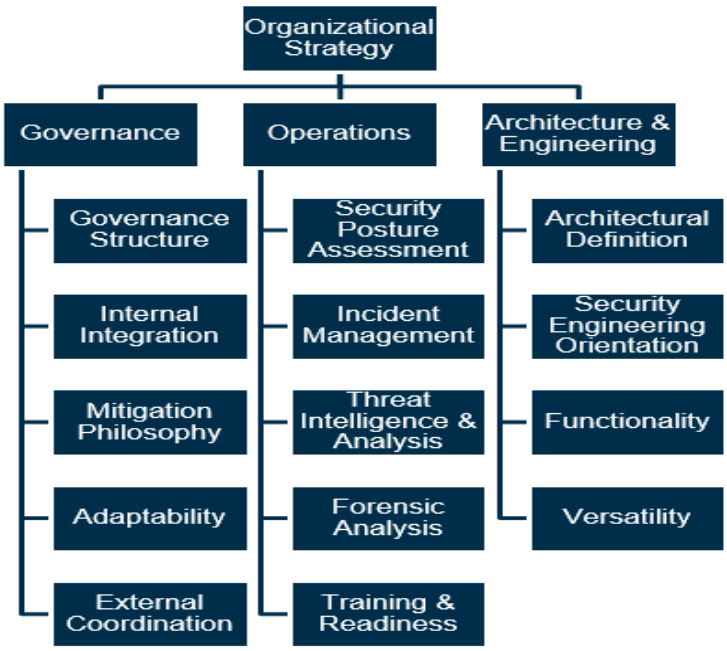

Figure 6. Aspects of Organizational Cyber Preparedness Strategy [Bodeau 2016]

Alternately, or in addition, an institution can be characterized using the draft Financial Services Sector Specific Cybersecurity "Profile" [FSSCC 2017b] [FSSCC 2017c]. That profile includes not only the functions from the NIST Cybersecurity Framework [NIST 2014] [NIST 2018], but also governance and supply chain / dependency management. Finally, an additional characterization of an institution's preparedness may be its Fair Isaac Corporation (FICO) Enterprise Security Score [FICO 2017]; the scoring system is a recent development, and its utility remains to be determined.

An adversary can use open source intelligence-gathering or insider knowledge to define an overall characterization of the cyber preparedness of the participant institutions. The adversary can then use this characterization for targeting and attack planning, taking into consideration how well a participant institution can be expected to ingest and use shared threat intelligence, how effectively it uses partnership or other relationships to respond to disruptions or suspected attacks, and how carefully it manages supply chain risks.

3.2.2 System-of-Systems Characteristics

Developing a system-of-systems attack scenario requires additional information beyond the threat events identified in the previously defined high-level threat model [Bodeau 2018]. At the individual FSS institution level, some attacks may be opportunistic and simply launch exploits on any technology or interface exhibiting a technical vulnerability. Others, specifically targeting the FSS institution, may have the goal of affecting a particular business function. The latter types of attacks require some information about where the function is located in the system and what security controls surround it.

At the system-of-systems level, however, the adversary's goal is either to leverage the relationships and dependencies in the system of systems for direct financial gain or indirect advantage (e.g., via a data breach), or – more problematically – to create systemic effects on a

sub-sector business function collaboratively done by interdependent systems at multiple FSS institutions. In this context, the attack likely needs to be crafted with cognizance of the structure and dynamics of the business function across the collection of institutions. The increased emphasis on how and where the contributing elements of the business process operate means that additional descriptive models are needed to guide the employment of threat events in the high-level threat model as part of a system-of-systems attack.

3.2.2.1 System-of-Systems Structural Model

In order to plan an effective attack at the system-of-systems level, an adversary needs to know what individual systems are constituents of the system of systems, how they are interconnected, where the processing components of the business function take place, and how they combine to form the sub-sector function. That is, the adversary needs to understand the structure of the system of systems, including its network topology, its normal information and control flows, and its information and control flows under stress or other contingencies. An adversary selects and tailors attack activities based on an understanding of the SoS structure.

The structure of a system of systems can be understood as an instance of a pattern [Kazman 2013]. System-of-systems patterns can be modeled at two layers: operational and system [Kalawsky 2013].

At the operational layer, a variety of network topologies can be identified for sub-sectors or institution-spanning functions. These include butterfly or bow-tie networks, in which one system (e.g., a common backbone) or a tight mesh of systems is central to all transactions [Battiston 2010] [Bardoscia 2017], core-periphery networks [Kajoku 2018], and mesh networks. All topologies are subject to attack propagation and cascading failures [Roukny 2013], but the selection and sequencing of attack events to maximize achievement of adversary goals will be different.

At the system layer, interactions between constituent systems can be represented and analyzed from different technical viewpoints, taking into consideration how constituent systems interact (e.g., via information exchange, behavior interaction or service use, complex behavior interaction or business logic, or a shared user interface [Kazman 2013]). Five broad patterns of SoS architectures have been identified: centralized (corresponding to a butterfly or hub-and-spokes network); service-oriented architecture (SOA); publish-subscribe; pipes-and-filters; and blackboard [Ingram 2014]. Identification of which system-level SoS architectural patterns are more susceptible to different adversary control strategies (see Section 3.2.1.1) or attack patterns (see Section 3.3.3) remains to be determined.

In addition to the underlying structure of the system-of-systems or sector function, an adversary can also examine the structure of the supply chains for constituent systems in general or for key constituent systems.

Finally, an adversary can take into consideration the types of relationships that have been established on the cyber defense side. (Note that Table 3, in Section 3.3.1, can be used to characterize relationships between organizations on the cyber defense side, including participant institutions, DHS, and law enforcement.)

3.2.2.2 System-of-Systems Cyber Defense Capabilities

An attack intended to disrupt a system-of-systems business function that is immediately and predictably stopped by the one or more of the constituent systems' cyber defenses is ineffective and pointless. In order to prevail, an attack scenario must be designed with at least general awareness of what cyber defenses the constituent systems are likely to have in place.

A representation of a system of systems' cyber defense capabilities identifies the minimal cybersecurity capabilities required or expected of constituent systems, additional capabilities allocated to specific constituent systems, and additional capabilities provided by selected constituent systems due to owning institutions' cyber risk management strategies. Minimal cybersecurity capabilities can be identified in terms of the Cybersecurity Assessment Tool (CAT) provided by the Federal Financial Institutions Examination Council (FFIEC) [FFIEC 2015].[9] Additional capabilities can be identified using the Cyber Resiliency Engineering Framework in the draft Volume 2 of NIST SP 800-160 [NIST 2018b] or the draft Financial Services Sector Specific Cybersecurity "Profile" [FSSCC 2017b] [FSSCC 2017c].

3.2.2.3 System-of-Systems Decision Model

Negative systemic behavior can sometimes occur through happenstance as a result of untoward circumstances and flaws in the system of systems, such as when error processing and failover at a site in a Midwestern electrical grid caused overloading at successive sites that then failed over to others in turn, resulting in a large-scale regional cascading power failure [NERC 2004]. But a cyber attacker aspiring to create a systemic disruption needs knowledge of how to exploit the system dynamics and manipulate its mitigations.

Bringing about an effect on the system-of-systems business function requires knowledge not just of the components and pathways discoverable from the structural model but also of information that characterizes the processing and control of the business function. This information might include, for instance, quantities, rates, and thresholds for successful operation and for triggering a control change or activation of a risk mitigation such as a temporary hold on processing. It might also include knowledge of error processing and failover. The decision model can be expressed in terms of a response and recovery lifecycle, as defined in [Gray 2018].

3.3 Threat Scenario Structure

A threat scenario is "a set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time." [NIST 2012] Thus, the specification or description of a threat scenario consists of a characterization of the adversary or adversaries taking action against a target (or target set), in terms of the adversary's capabilities, intent, and targeting considerations; and a partially ordered set of threat events. The structure of a threat scenario for a system of systems differs from that of a scenario for a single system or an institution in its treatment of adversaries, description of threat events, and general patterns.

[9] See [Fox 2018c] for an example of how an institution can profile its defensive capabilities.

3.3.1 Represent Multiple Adversaries

In a system-of-systems threat scenario, multiple threat actors can be involved. Often, one adversary can be identified as the leader or orchestrating actor, engaging other threat actors for the execution of specific threat events and coordinating their activities. In some system-of-systems threat scenarios, the orchestrating actor has and maintains relationships with the other actors. This is particularly the case for scenarios in which a nation-state actor coordinates or directs the activities of criminal enterprises. In other scenarios, the orchestrating actor does not actively engage with the other actors, but offers resources such as malware or intelligence information about institutions they want targeted; the other actors (e.g., criminal actors with access to a venue in which the resources are provided) simply act in accordance with their own interests.

Therefore, the description of a system-of-systems threat scenario can separately characterize the orchestrating actor, the other actors, and their relationships. Relationships can be characterized along a spectrum, as shown in Table 3 (adapted from [Bodeau 2014]).

Table 3. Spectrum of Relationships

Relationship Level	Description (Bold indicates differences between levels)
Collaboration	The two parties plan for, allocate resources to, and **jointly** manage activities to achieve a common goal or address a common problem; these activities are designed to avoid impeding or negating each other's efforts.
Coordination	The two parties **plan for, allocate resources to, and manage separate activities** to achieve the **common** goal or address the **common** problem; **these activities are designed** to avoid impeding or negating each other's efforts.
Cooperation	The two parties seek to **achieve the goal or address the problem, and** to avoid impeding or negating each other's efforts.
Deconfliction	The two parties **seek to avoid impeding or negating each other's efforts to address the problem**.
Communication	The two parties **communicate or share information with each other regarding** the problem.
Mutual Indifference	**The two parties are either unaware of or indifferent to each other's activities.**
Observation	The two parties **observe each other's activities.**
Frictional Conflict	**The activities by one party impede or negate the intended effects of activities by the other party.**
Competition	The two parties **seek to achieve competing or mutually exclusive goals.**
Contention (or Contestation)	The two parties **vie for control of or dominance over a set of resources.**
Coercion	**One party seeks to coerce the other into submitting to specific demands.**

3.3.2 Contextualize Threat Events

The description of a threat event can be high-level (as in Table 15 of [Bodeau 2018]), can provide more narrative detail (as in [NSA 2018]), or can identify specific TTPs from a repository or taxonomy such as Adversarial Tactics, Techniques, and Common Knowledge™ (ATT&CK™) or CAPEC™ (as in Table 5 of [Fox 2018b]). For a threat scenario targeting a

single system or institution, the description of a threat event can be contextualized by identifying the assets targeted or affected by the threat event and the event's cyber effects on those assets. A threat event can also be contextualized in terms of timing – i.e., whether the event is more likely to succeed at certain times or under certain conditions. For a system-of-systems threat scenario, the description of a threat event can be contextualized by identifying (i) constituent systems or participant institutions targeted or affected by the threat event, (ii) constituent systems or technologies exploited in the execution of the threat event, (iii) the event's effects on the sector function, participant institutions, and constituent systems, and (iv) timing.[10]

3.3.3 Recognize Patterns of Systemic Cyber Attack

One structure of a threat scenario involving a single system or institution is defined in NIST SP 800-30R1 [NIST 2012], consistent with a broad set of cyber attack lifecycle or cyber kill chain models.[11] In that structure, adversary activities follow a general sequence of reconnaissance, weaponization, delivery, exploitation, control, execution, and maintenance. While originally defined for an individual system or enterprise information infrastructure, that structure can also be applied to a system of systems.

A number of patterns of attacks to create systemic consequences on a sector or sub-sector business function of a system of systems can be identified by surveying the published literature on such attacks (see, for example, [Maurer 2017]), by analyzing the representative topologies or system-of-systems structural models (see Section 3.2.2.1), and by surveying prior work on system-of-systems cyber threat modeling (see Section 2.3). Table 4 identifies an initial set of patterns. The description of each pattern indicates the targeting scope (see Table 1) and adversary control strategy (see Section 3.2.1.1) which best fit that pattern.

Table 4. Initial Set of Patterns of Systemic Cyber Attack

Pattern	Description	Examples / References
Common mode / repeated attack	Attack multiple constituent systems or participant institutions by exploiting a technology they all use Scope: Technically narrow and/or institutionally narrow Control: Loosely directed	The FIN7 criminal group's use of Carbanak [Williamson 2015] [Riley 2017] Attacks on institutions relying on SWIFT [Schwartz 2016]
Common mode / scattershot attack	Attack multiple systems or participant institutions without coordination or orchestration, by exploiting a technology they all use Scope: Technically narrow Control: Contagion-based	Watering-hole attack [Symantec Security Response 2017]

[10] For example, the transfer requests in the Bangladesh Central Bank heist were timed to take advantage of the time difference between Bangladesh and New York City. [Maurer 2017]

[11] See Section 2.1.5.3 of [Bodeau 2018] for a survey.

Pattern	Description	Examples / References
Common mode / pervasive attack	Attack many or all constituent systems individually simultaneously or in an orchestrated sequence of activities, exploiting a technology they all use Scope: Technically narrow, institutionally broad Control: Closely directed	Quantum Dawn IV scenario [SIFMA 2017] 2012-2013 DDoS attacks on websites (disrupting commercial online banking) [Maurer 2017] Induce a pervasive failure in a major software application [Saydjari 2010] (scenario 1)
Rolling attack	Attack primary and alternative systems sequentially, to disrupt the sector function or to continue achieving objectives (e.g., large-scale theft) Scope: Institutionally narrow Control: Closely directed	Quantum Dawn III scenario – rolling attacks on equity exchanges [SIFMA 2017] Ongoing DarkSeoul attacks [Pagliery 2017] DDoS attacks using a leased or acquired botnet [Moriuchi 2018]
Transitive attack	Conduct an attack on a constituent system upstream in the business function process of the ultimate target Scope: Functionally narrow and/or institutionally narrow Control: Closely directed	Attack a weak-link payment processor [Brenner 2017] to enable attacks on payment systems in participating institutions
Cascading attack	Attack in such a way that as the attack spreads to additional victims, its effects get worse (e.g., due to compounding effects of error handling in successive systems) Scope: Technically narrow Control: Contagion-based	Implied by concerns for interconnectedness [Bank of Canada 2017] Exploit an unrecognized dependency [Saydjari 2017] (scenario 5)
Shared resource consumption attack	Conduct attacks on multiple constituent systems that create demands on a shared resource to the extent that it cannot meet the levels needed by all participant institutions Scope: Technically narrow and/or functionally narrow Control: Loosely directed	Coordinated DDoS attacks Overwhelm a multi-institution recovery site [Saydjari 2017] (scenario 9)
Critical function attack	Attack a function, such as an exchange or clearing function, that all participants use Scope: Functionally narrow Control: Closely directed	Clearing house scenarios [SIFMA 2017] [Saydjari 2017] (scenario 12) Nasdaq hack [Riley 2014]

Pattern	Description	Examples / References
Regional attack	Attack a sector function by attacking resources in a specific geographic region Scope: Functionally narrow Control: Closely directed	Attack the major data centers for processing credit card transactions on the East Coast [Saydjari 2017] (scenario 7)
Service dependency attack	Attack an underlying service on which multiple participants rely Scope: Technically narrow and/or functionally narrow Control: Closely directed	Attack a financial processing service vendor Attack an IT service layer (e.g., Dyn DDoS attack) Attack a critical infrastructure, like communications or electricity [Saydjari 2017] (scenario 3)
Coordinated supply chain attack	Attack one or more components of the supply chain providing IT to constituent systems Scope: Technically narrow and/or functionally narrow Control: Closely directed	Attack or subvert vendors involved in designing, manufacturing, and distributing hardware and software [Saydjari 2017] (scenario 2) Attack or subvert vendors performing diagnostics and maintenance of hardware and software Attack or subvert vendors involved in ongoing work or support as part of the operation of the production system.

Alternately, threat scenarios can be defined by exploring the seven aggregations of cyber risk identified in [Zurich Insurance 2014]: institution-internal IT, counterparties and partners, outsourced and contract, supply chain, disruptive technologies, upstream infrastructure, and external shock. For example, transitive or cascading attacks leverage institution-internal, counterparties and partners, and outsourced and contract risks.

4 Developing System-of-Systems Threat Scenarios

This section describes a general process for developing threat scenarios for systems of systems. It illustrates how the general threat modeling framework can be used to develop a threat scenario from a sector-level or an institution-centric view. It describes how such a threat scenario could be used.

A scenario can be characterized in simple terms of its target and its intended effects, as shown in Table 5. (This table abstracts and summarizes material from Table 1.)

Table 5. Enterprise vs. System-of-Systems Attacks

		Extent of Effects	
		Narrow/Localized	Broad
Target	Single FSS institution	Business function within the institution	Set of institutions partnered with or dependent on target institution
	Multiple FSS institutions	Business function spanning multiple institutions	Systemic: sub-sector, region, set of institutions sharing a common infrastructure or service

An attack on a single FSS institution would most often have local effects, though it is possible to identify examples that could have systemic effects, depending on the type of institution or the type of attack (e.g., loss of market confidence due to modification of requested trades). An attack on multiple members of an interdependent system of systems could, by the same token, potentially have only localized effects on the constituent systems. However, the attacks of greatest interest for system-of-systems scenarios are those that involve multiple members of the system of systems as targets and are intended to have systemic effects. They attack multiple targets to achieve a coherent business function-oriented adversary goal.

4.1 Scenario Development Process

While it was applied to the electrical power sector, the scenario design and threat modeling approach developed by Lloyd's [Lloyd's 2015] can be applied more generally. In this approach, the network structure of the sector, sub-sector, or business function is briefly characterized (e.g., horizontal, vertical, hub-and-spoke). The primary attacker's motivation is identified, and used to determine the choice of target regions, functions, or institutions. The attacker's motivation is also used to determine the class of threat scenario consequences to consider (e.g., disruption of service delivery).[12]

[12] In the Lloyd's process, statistical data about potential targets is obtained to determine their relative criticality. An analysis is then performed on historical data of extreme events in the relevant threat scenario class, to identify their observed impacts; this enables estimates of economic losses to be generated.

The Lloyd's process is augmented as follows: The primary or lead adversary is profiled in more detail, consistent with the hTMM process, using the framework described in [Bodeau 2018] as extended in Section 3. Thus, the adversary's intent is characterized in terms of principal motivation (e.g., systemic disruption) and secondary or additional motives (e.g., financial gain; reputation damage to an institution, a set of institutions, a sector, or a nation); the scope or scale of the adversary's activities (see Table 1); the intended or expected cyber effects and institutional consequences associated with the adversary achieving their goals; the timeframe in which the adversary operates; the adversary's degree of persistence and concern for stealth; and the adversary's opportunism. In addition to profiling the primary or lead adversary, additional threat actors are also profiled. Relationships between the lead adversary and the secondary threat actors are characterized using Table 3.

A representative set of historical examples can be used as reference, and a pattern of system-of-systems attack which reflects the network structure can be selected from Table 4.

4.2 Representative Example

A representative example of a system-of-systems threat scenario is provided in this section. It involves an attack on the credit card processing function, within the deposit, consumer credit, and payment systems sub-sector. As discussed in Section 2.2.1, many system-of-systems functions in the financial sector could be the subject of threats and attack scenarios, including brokerage/trading, funds transfer, ATM networks, mobile payment systems, and others. However, credit card processing offers several characteristics which illuminate the relationship between attacks on constituent systems and on the overall sub-sector function.

The subsections below follow the process described in Section 4.1. First, the network structure of the targeted function is described. Second, adversary profiles are defined for the scenario. Finally, a scenario is described.

4.2.1 Credit Card Processing System of Systems

Figure 7 shows the flow of interactions among participating institutions to process authorization and payment of a credit card transaction.[13]

[13] For more detail, see [Herbst-Murphy 2013].

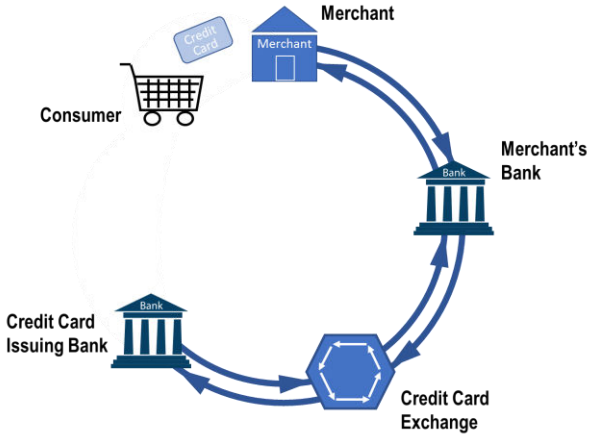

Figure 7. Credit Card Processing Flow

When a transaction occurs, these FSS participating institutions collaborate to authorize the transaction and then forward payment. The credit card information and transaction amount are sent to the merchant's bank, also known as the acquiring bank. The merchant's bank then forwards the transaction information via a credit card exchange such as the Visa, Mastercard, and American Express (AMEX) networks to the credit card issuing bank, which authorizes the transaction and passes funds back through the credit card exchange to the merchant's bank.

As shown in Figure 8, a large bank typically has business functions to serve the roles of both the acquiring bank for merchants and the issuing bank for credit cards. The online credit card and banking applications shown in the upper left serve customers for whom the bank is the credit card issuing bank. The merchant authorization and clearing function in the lower left processes transactions from merchants for whom the bank is the acquiring bank. The card business application controls the processing, as appropriate, to:

- send or receive and respond to authorization requests via the card authorization transaction gateway
- send or receive funds over one of the payment networks to settle the transaction via the transaction settlement function.

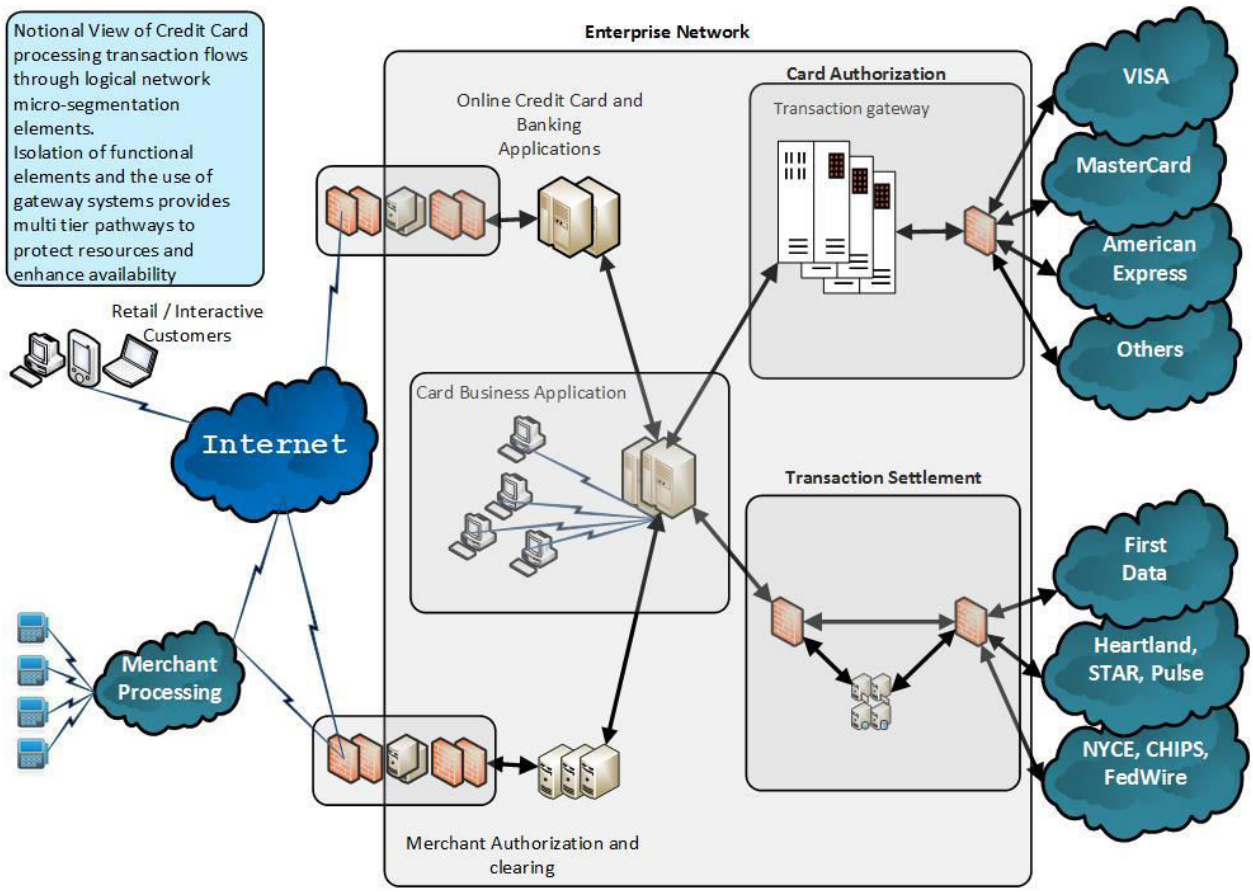

Figure 8. Credit Card Processing in a Representative Bank

As shown in highly simplified form in Figure 9, a system of systems performing card processing is formed of many banks, each with its own merchant and credit card customers, interacting in a hub-and-spoke structure with a credit card exchange to authorize and settle transactions.

Figure 9. Network Topology for Credit Card Processing

4.2.2 Adversary Profiles

The primary, lead, or orchestrating adversary is a nation-state actor that would like to undermine public confidence in the U.S. financial system to enhance its ability to apply pressure in an international economic negotiation. This actor targets credit card processing as central to the experience of the financial sector shared by a broad consumer population. The adversary chooses to operate at a scale which is technically and institutionally broad, but functionally localized (to credit card processing, rather than, for example, all functions within the deposit, consumer credit, and payment systems sub-sector). The primary adversary seeks reputation damage to participant institutions, the sub-sector, and government agencies involved in mitigating and redressing the attack. Intended cyber effects are primarily degradation or interruption of service; however, threat actions in the scenario will produce a wide range of cyber effects on constituent systems.

The primary adversary orchestrates activities over an extended period, perhaps a year or more, when intelligence-gathering, planning, and resource development activities are included. The adversary is highly persistent, and has a high concern for stealth.[14] The primary adversary has access to sophisticated cyber attack capabilities including zero-days, and substantial resources in the form of funding and staffing, and is able, if necessary, to prepare, weaponize, and conduct attacks over long periods of time.

The primary adversary makes use of two additional actors:

- Criminal Group 1: this criminal group develops and sells exploits for merchant credit card processing infrastructure. It has moderate cyber capabilities, and operates on a one-time basis.
- Criminal Group 2: this criminal group is known to perpetrate credit card fraud. It is motivated by financial gain, does not have sophisticated cyber capabilities, and operates on a one-time or episodic basis.

The principal threat actor's relationship with both criminal groups is communication (see Table 3).

4.2.3 Attack Scenario

The primary adversary sets the goals of:

- disrupting credit card operations on dates when high volumes of transactions occur and that are psychologically important to businesses and consumers;
- maintaining the disruption over a period of days; and
- making it difficult to determine what has gone wrong.

The adversary sets a strategy with multiple teams carrying out components of a large-scale coordinated attack. A lead actor directs and tasks the teams for which specific targets to attack when.

Well in advance, the adversary prepares and weaponizes elements of the attack:

[14] In terms of Table 10 of [Bodeau 2018], the adversary's activities are *sustained* or *enduring*.

- finds or creates a zero-day attack using a previously unknown vulnerability in the operating software of widely used routers and switches;
- surreptitiously acquires large volumes of active credit card numbers and consumer identities, complete with credit card validation numbers, either on the black market or through long-term intrusions into point-of-sale systems to harvest credit cards;
- develops malware capable of exploiting the credit card processing systems used at many banks; and
- commissions Criminal Group 1 to develop and insert malware that exploits a vulnerability in a popular on-line shopping cart and check-out software system used by many merchants. The malware remains dormant until triggered. Criminal Group 1 has no knowledge of how, when, or by whom its exploit will be used.

The adversary plans and directs the attack as follows:

- Shortly before the planned attack, Teams 1 and 2 are each assigned to implant the credit card processing systems malware into the credit card processing systems of three major issuing banks, half a dozen total.
- On Black Friday, Team 2 exploits the router and switch vulnerability to bring down the network infrastructure for the data centers that process credit card transactions for the East Coast.[15] The attack is disruptive, particularly on a day critical to merchants and consumers, but appears regional and the industry hopes to diagnose and resolve it quickly.
- The lead actor follows the recovery efforts closely, using both public reports in the press and tools designed to probe the systems to determine their status. The lead actor instructs Team 2 to look for opportunities to re-insert the exploit into recovered systems and back-ups.
- On the weekend, Teams 1 and 2 trigger the credit card processing malware at their assigned banks in a time-phased sequence, which makes the attack first appear to be institution-specific but quickly proves to involve other banks. The malware causes pervasive failure of credit card transaction authorization and payments processing. The problem is now national. Credit card transactions above the off-line authorized dollar limit are refused. Issuing and acquiring banks and the credit card network work intensely to identify the cause. Once it becomes clear the disruption is due to a cyber attack, banks take systems off-line, attempting to find and eradicate the malware. The disruption to credit card transactions, due to both the attack itself and the efforts to recover, is extremely visible and frightening to the public. Credit card processing has been repeatedly disrupted now for a period of days, and consumers, journalists, and the government are raising alarms and pressing for action.
- Over the weekend, the lead actor (or a surrogate) provides Criminal Group 2 with the harvested credit card information and access to the on-line shopping cart system exploit

[15] See [Kontzer 2013] for a description of Visa's Operations Center East.

purchased from Criminal Group 1. Criminal Group 2 has no knowledge of the source of the exploit.

- On Cyber Monday, the peak day for on-line shopping, Criminal Group 2 launches huge numbers of fraudulent on-line credit card transactions to both prominent and small retailers, using the acquired credit card numbers. Chip-and-signature cards offer no defense against on-line fraud, as they can provide extra safeguards only when used in point-of-sale terminals. Consumers enrolled in text alerting services for on-line transactions receive alerts for purchases they did not make and contact their credit card issuers to report them. The wave of fraudulent transactions rapidly becomes known. Consumer and merchant confidence drops drastically. Many switch to cash transactions, putting burdens on the cash supplies in the ATM system. After several days of disruption in multiple component systems, using multiple modes of attack, even when systems return to normal and the wave of fraud trails off, confidence is slow to return.

This threat scenario involves effects on constituent systems in the credit card processing system of systems, including

- Systems at East Coast credit card processing data centers: denial-of-service (degradation, interruption) via exploitation of router and switch vulnerability;
- Credit card authorization and transaction settlement systems at three major card issuing banks: denial-of-service (degradation, interruption) via triggered malware; and
- Credit card authorization and transaction settlement systems at three major card issuing banks: corruption of transaction data via fraudulent transactions.

This threat scenario is an initial example, serving to illustrate an attack where both the targets and the effects extend to multiple interrelated institutions participating in a system of systems. However, it is incomplete insofar as it does not represent the role of institutional cyber preparedness, the SoS cyber defense model, and the SoS decision model in the adversary's attack strategy.

5 Conclusion

This report is an initial step toward defining and using a structured approach to developing system-of-systems cyber threat scenarios. This report has extended a cyber threat modeling framework developed for individual institutions in the financial services sector to support development of system-of-systems cyber threat scenarios. The feasibility of using the extended framework is demonstrated by developing a representative example scenario.

Several uses can be made of a system-of-systems cyber threat scenario, and hence of the extended framework described in this report:

- A system-of-systems scenario can be used in a large-scale (multi-institutional) cyber exercise or cyber wargame. The extended framework can be used to structure the description of the scenario and to improve its internal consistency and completeness.
- A large-scale cyber exercise may include not only a systemic attack, but also attacks at participating institutions. The extended framework provides a link between the description of the systemic scenario and the more detailed scenarios specific to different participating institutions.
- A system-of-systems scenario can be used in modeling and assessment of systemic risks. The extended framework provides representative values for factors which could be used in the risk assessment process. In particular, because a system-of-systems scenario can involve multiple threat actors, the characterization of relationships among those actors can be useful in modeling and assessment.
- Reported incidents and postulated attacks can be analyzed using the extended framework.

As next steps, the system-of-systems threat model should be further refined by developing an example of how a SoS threat scenario can be integrated with an institution-specific scenario (e.g., by identifying a high-level threat event in a SoS threat scenario with a threat scenario for a constituent system or participating institution); exploring ways to represent institutional cyber preparedness, the SoS cyber defense model, and the SoS decision model in the threat scenario development and presentation; and developing some examples of novel threat scenarios.

List of Acronyms

Acronym	Definition
AMEX	American Express
ATM	Automated Teller Machine
ATT&CK™	Adversarial Tactics, Techniques, and Common Knowledge
BEC	Business Email Compromise
BITS	Banking Industry Technology Secretariat
C2	Command and Control
CAPEC™	Common Attack Pattern Enumeration and Classification
CAT	(FFIEC) Cybersecurity Assessment Tool
CHEW	Criminals, Hacktivists, Espionage, War
CHIPS	Clearing House Interbank Payments System
CI	Critical Infrastructure
COBIT	Control Objectives for Information and Related Technologies
COOP	Continuity of Operations
CSS	Central Security Service
DACS	Describing and Analyzing Cyber Strategies
DBMS	Database Management System
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DNS	Domain Name System
DoS	Denial of Service
DTCC	Depository Trust & Clearing Corporation
ENISA	European Union Agency for Network and Information Security
FBIIC	Financial and Banking Information Infrastructure Committee
FFIEC	Federal Financial Institutions Examination Council
FFRDC	Federally Funded Research and Development Center

Acronym	Definition
FICO	Fair Isaac Corporation
FNDA	Functional Network Dependency Analysis
FS-ISAC	Financial Sector Information Sharing and Analysis Center
FSS	Financial Services Sector
FSSCC	Financial Services Sector Coordinating Council
FSTC	Financial Services Technology Consortium
HSSEDI	Homeland Security Systems Engineering & Development Institute
hTMM	(SEI) Hybrid Threat Modeling Method
IEC	International Electrotechnical Commission
IEEE	Institute for Electrical and Electronics Engineers
IIF	Institute of International Finance
IMF	International Monetary Fund
ISO	International Organization for Standardization
IT	Information Technology
JTC	Joint Technical Committee
M&S	Modeling and Simulation
NCSC	National Cyber Security Centre (Netherlands)
NERC	North American Electric Reliability Council
NGCI	Next Generation Cyber Infrastructure
NIST	National Institute of Standards and Technology
NMS	National Market System
NSA	National Security Agency
NYCE	New York Currency Exchange
ODNI	Office of the Director of National Intelligence
OFR	Office of Financial Research
OS	Operating System

Acronym	Definition
OWASP	Open Web Application Security Project
PASTA	Process for Attack Simulation & Threat Analysis
PII	Personally Identifiable Information
PnG	Persona non Grata
S&T	Science and Technology Directorate
SEI	Software Engineering Institute at Carnegie Mellon University
SIFMA	Securities Industry and Financial Markets Association
SOA	Service-Oriented Architecture
SOC	Security Operations Center
SoS	System of Systems
SP	(NIST) Special Publication
STRIDE	(Microsoft) Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAL	(Intel) Threat Agent Library
TARA	(Intel) Threat Agent Risk Assessment (MITRE) Threat Assessment and Remediation Analysis
TTP	Tactics, Techniques, and Procedures

List of References

1. Ablon, L., Libicki, M.C., and Golay, A.A. 2014. "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar," The RAND Corporation, June 19, 2014. http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

2. AIG. 2017. "Is cyber risk systemic?" May 9, 2017. https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aig-cyber-risk-systemic-final.pdf.

3. Allen, F., and Babus, A. 2009. "Networks in Finance," in *The Network Challenge: Strategy, Profit, and Risk in an Interlinked World*, Upper Saddle River, NJ, Wharton School Publishing, 2009, pp. 367-382.

4. Alvarez, M. 2017. "Security trends in the financial services sector," IBM X-Force Research. April 25, 2017. https://media.scmagazine.com/documents/296/2017_ibm_x-force-_security_tre_73846.pdf.

5. Bank of Canada. 2017. "Financial System Review," June 2017. https://www.bankofcanada.ca/wp-content/uploads/2017/06/fsr-june2017.pdf.

6. Bank of England. 2016. "CBEST Intelligence-Led Testing, An Introduction to Cyber Threat Modelling, Version 2.0," The Bank of England, 2016. http://www.bankofengland.co.uk/financialstability/fsc/Documents/anintroductiontocbest.pdf.

7. Bardoscia, M., Battiston, S., Caccioli, F., and Cardarelli, G. 2017. "Pathways towards instability in financial networks," Nature Communications, February 17, 2017. https://www.nature.com/articles/ncomms14416.

8. Battiston, S., Glattfelder, J.B., Garlaschelli, D., Lillo, F., and Caldarelli, G. 2010. "The Structure of Financial Networks," in *Network Science: Complexity in Nature and Technology*, pp. 131-163, London, Springer-Verlag, 2010.

9. Bodeau, D., Brtis, J., Graubart, R., and Salwen, J. 2013. "Resiliency Techniques for System of Systems: Extending and Applying the Cyber Resiliency Engineering Framework to the Space Domain," MTR 130515, PR 13-3513, September 2013. http://www.mitre.org/sites/default/files/publications/13-3513-ResiliencyTechniques_0.pdf.

10. Bodeau, D., and Graubart, R. 2014. "A Framework for Describing and Analyzing Cyber Strategies and Strategic Effects," MTR 140346, PR 14-3407, The MITRE Corporation, 2014.

11. Bodeau, D., and Graubart, R. 2016. "Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms of Preparedness," MTR 150264, PR 16-0939, The MITRE Corporation, 2016.

12. Bodeau, D., McCollum, C., and Fox, D. 2018. "Cyber Threat Modeling: Survey, Assessment, and Representative Framework," PR 18-1174, HSSEDI, The MITRE Corporation, 2018.

13. Boer, M., and Vazquez, J. 2017. "Cyber Security & Financial Stability: How cyber-attacks could materially impact the global financial system," Institute of International Finance, September 2017. https://www.iif.com/system/files/iif_cyber_financial_stability_paper_final_11_13_2017_clean.pdf.

14. Brenner, J. 2017. "Keeping America Safe: Toward More Secure Networks for Critical Sectors - Report on a Series of MIT Workshops, 2015-2016," March 2017. https://cis.mit.edu/sites/default/files/documents/Report-IPRI-CIS-CriticalInfrastructure-2017-Brenner.pdf.

15. Caralli, R.A., et al. 2007. Carnegie Mellon University - Software Engineering Institute, "OCTAVE Allegro: Improving the Information Security Risk Assessment Process," May 2007. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419 or http://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

16. Carter, W.A. 2017. "Forces Shaping the Cyber Threat Landscape for Financial Institutions," SWIFT Institute Working Paper No. 2016-004, October 2, 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/171006_Cyber_Threat_Landscape%20_Carter.pdf.

17. Center for Homeland & Cyber Security, The George Washington University. 2017. "Cybersecurity in the Financial Services Sector: Issue Brief 4 in a Series Based on Fall 2017 Symposium Proceedings," November 13, 2017. https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/DT%20panel%204%20issue%20brief%20final.pdf.

18. Cliff, D., and Northrop, L. 2011. "The global financial markets: an ultra-large-scale systems perspective," 7 September 2011. https://pdfs.semanticscholar.org/e507/e211f6490382bd23396a3ba9299f88214855.pdf.

19. Dahmann, J.S., Rebovitch, G.J., and Turner, G.N. 2015. "Security Engineering in a System of Systems Environment," in *20th International Command and Control Research and Technology Symposium*, Annapolis, MD, 2015.

20. Danielsson, J., Fouché, M., and Macrae, R. 2016. "Cyber risk as systemic risk," Vox - the policy portal for the Centre for Economic Policy Research, June 10, 2016. https://voxeu.org/article/cyber-risk-systemic-risk.

21. de Bruijne, M., van Eeten, M., Hernández Gañán, C., and Pieters, W. 2017. "Towards a new cyber threat actor typology: A hybrid method for the NCSC cyber security assessment," August 30, 2017. https://www.wodc.nl/binaries/2740_Samenvatting_tcm28-273245.pdf.

22. Deloitte. 2015. "Standing Together for Financial Industry Resilience: Quantum Dawn 3 After-Action Report," Deloitte, November 19, 2015. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-quantum-dawn-3-after-action-report.pdf.

23. Defense Acquisition University. 2013. "Defense Acquisition Guidebook (2013)," Defense Acquisition University, September 16, 2013. https://acc.dau.mil/docs/dag_pdf/dag_complete.pdf.

24. DTCC, "Cyber Risk – A Global Systemic Threat," Depository Trust & Clearing Corporation, October 2014. http://www.dtcc.com/~/media/Files/Downloads/issues/risk/cyber-risk.pdf

25. ENISA. 2017. "Ransom attacks against unprotected Internet exposed databases," European Union Agency for Network and Information Security, September 13, 2017. https://www.enisa.europa.eu/publications/info-notes/ransom-attacks-against-unprotected-internet-exposed-databases.

26. FFIEC. 2015. "FFIEC Cybersecurity Assessment Tool," OMB Control 1557-0328, Federal Financial Institutions Examination Council, June 2015. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf.

27. FICO. 2017. "FICO Enterprise Security Score: The Science of Cybersecurity Predictive Analytics," Fair Isaac Corporation, 1 June 2017. http://www.fico.com/en/node/8140?file=12697.

28. Fox, D., McCollum, C., Arnoth, E., and Mak, D. 2018. "Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context," PR 18-1636, HSSEDI, The MITRE Corporation, 2018.

29. 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," PR 18-1725, HSSEDI, The MITRE Corporation, 2018.

30. Fox, D., Arnoth, E., Skorupka, C., and McCollum, C. 2018c. "Enterprise Threat Model Technical Report: Cyber Threat Model for a Notional Financial Services Sector Institution," PR-1613, HSSEDI, The MITRE Corporation, 2018.

31. FSSCC. 2017. "Financial Services Sector Cybersecurity Recommendations," Financial Services Sector Coordinating Council, January 18, 2017. https://www.fsscc.org/files/galleries/FSSCC_Cybersecurity_Recommendations_for_Administration_and_Congress_2017.pdf.

32. FSSCC. 2017b. "Financial Services Sector Specific Cybersecurity 'Profile'," Financial Services Sector Coordinating Council, NIST Cybersecurity Workshop, May 27, 2017. https://www.nist.gov/sites/default/files/documents/2017/05/18/financial_services_csf.pdf.

33. FSSCC. 2017c. "The Financial Services Sector Specific Cybersecurity Profile - Description, Benefits, and Intent, DRAFT v3.1," Financial Services Sector Coordinating Council, 2017. http://www.fsroundtable.org/wp-content/uploads/2017/10/DRAFT-FS-Profile-Glossary-v3.1-Distro-NIST.xlsx.

34. FSSCC and FBIIC. 2015. "Financial Services Sector-Specific Plan 2015," 2015. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-financial-services-2015-508.pdf.

35. Garvey, P.R., and Pinto, C.A. 2012. *Advanced Risk Analysis in Engineering Enterprise Systems*, New York, NY, CRC Press, 2012.

36. Gray, A., and Mee, P. 2018. "Large-Scale Cyber-Attacks on the Financial System: A Case for Better Coordinated Response and Recovery Strategies," Depository Trust & Clearing Corporation and Oliver Wyman, March 2018. http://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2018/march/Large-Scale-Cyber-Attacks-DTCC-2018.pdf.

37. Guariniello, C., and DeLaurentis, D. 2014. "Communications, information, and cyber security in Systems-of-Systems: Assessing the impact of attacks through interdependency analysis," *Procedia Computer Science,* vol. 28, p. 720 – 727, 2014.

38. Herbst-Murphy, S. 2013. "Clearing and Settlement of Interbank Card Transactions: A MasterCard Tutorial for Federal Reserve Payments Analysts," October 2013. https://www.philadelphiafed.org/-/media/consumer-finance-institute/payment-cards-center/publications/discussion-papers/2013/D-2013-October-Clearing-Settlement.pdf.

39. HSSEDI. 2018. "Financial System Mapping (PR-1703)," The MITRE Corporation, 2018.

40. Infosec Institute. 2017. "MASSCAN - Scan the Internet in Minutes," Infosec Institute, March 24, 2017. http://resources.infosecinstitute.com/masscan-scan-internet-minutes/#gref.

41. Ingram, C., Payne, R., Perry, S., Holt, J., Hansen, F.O., and Couto, L.D. 2014. "Modelling Patterns for Systems of Systems Architectures," in *Eighth Annual IEEE Systems Conference*, Ottawa, ON, 2014.

42. Intel. 2007. "Threat Agent Library Helps Identify Information Security Risks," September 2007. https://communities.intel.com/docs/DOC-23853.

43. ISACA. 2009. "The Risk IT Framework," 2009. http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fmk_Eng_0109.pdf.

44. ISACA. 2012. "COBIT Version 5," April 2012. http://www.isaca.org/cobit.

45. ISO. 2015. "ISO/IEC JTC 1/SC 7, ISO/IEC/IEEE 15288:2015 - Systems and software engineering -- System life cycle processes," International Organization for Standarization, 2015.

46. Kalawsky, R.S., Joannou, D., Tian, Y., and Fayoumi, A. 2013. "Using architecture patterns to architect and analyze systems of systems," in *Conference on Systems Engineering (CSER'13)*, Atlanta, GA, 2013.

47. Kavak, H., Padilla, J.J., Vernon-Bido, D., Gore, R.J., and Diallo, S.Y. 2016. "A Characterization of Cybersecurity Simulation Scenarios," in *Proceedings of the 19th Communications & Networking Symposium*, Pasadena, CA, 2016.

48. Kazman, R., Nielsen, C., and Schmid, K. 2013. "Understanding Patterns for System-of-Systems Integration," Carnegie Mellon University Software Engineering Institute, December 2013. http://repository.cmu.edu/cgi/viewcontent.cgi?article=1771&context=sei.

49. Kojaku, S., Cimini, G., Caldarelli, G., and Masuda, N. 2018. "Structural changes in the interbank market across the financial crisis from multiple core-periphery analysis," February 14, 2018. https://arxiv.org/pdf/1802.05139.pdf.

50. Kontzer, T. 2013. "Inside Visa's Data Center," Network Computing, 29 May 2013. https://www.networkcomputing.com/networking/inside-visas-data-center/1599285558.

51. Kopp, E., Kaffenberger, L., and Wilson, C. 2017. "IMF Working Paper: Cyber Risk, Market Failures, and Financial Stability (WP/17/185)," August 2017. http://www.imf.org/~/media/Files/Publications/WP/2017/wp17185.ashx.

52. Lewis, D. 2017. "The DDoS Attack Against Dyn One Year Later," Forbes, October 23, 2017. https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attack-against-dyn-one-year-later/#58de89af1ae9.

53. Lloyd's. 2015. "Business Blackout - Appendix 2: Scenario design and impact modeling methodologies," July 6, 2015. http://www.lloyds.com/ScenarioDesign.

54. Lorenz, J., Battiston, S., and Schweitzer, F. 2009. "Systemic Risk in a Unifying Framework for Cascading Processes on Networks," *European Physical Journal B,* vol. 71, no. 4, p. 441–460, 2009.

55. Maier, M. 1998. "Architecting Principles for Systems of Systems," *Systems Engineering,* vol. 1, no. 4, pp. 267-284, 1998.

56. Maurer, T., Levite, A., and Perkovich, G. 2017. "Toward a Global Norm Against Manipulating the Integrity of Financial Data," Carnegie Endowment for International Peace, March 27, 2017. http://carnegieendowment.org/2017/03/27/toward-global-norm-against-manipulating-integrity-of-financial-data-pub-68403.

57. Mead, N.R., Shull, F., Vemuru, K., and Villadsen, O. 2018. "A Hybrid Threat Modeling Method," CMU/SEI-2018-TN-002, Carnegie Mellon University Software Engineering Institute,

March 2018. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2018_004_001_516627.pdf.

58. Microsoft. 2005. "The STRIDE Threat Model," 2005. http://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

59. The MITRE Corporation. "Common Attack Pattern Enumeration and Classification, A Community Resource for Identifying and Understanding Attacks," http://capec.mitre.org.

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

61. The MITRE Corporation. 2016. "Crown Jewels Analysis," MITRE Systems Engineering Guide, The MITRE Corporation. http://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis.

62. Moriuchi, P., and Chohan, S. 2018. "Mirai-Variant IoT Botnet Used to Target Financial Sector in January 2018," Recorded Future, April 5, 2018. https://www.recordedfuture.com/mirai-botnet-iot/.

63. NERC. 2004. "Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?" North American Electric Reliability Council, July 2004. https://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf.

64. NIST. 2011. "NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View," March 2011. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

65. NIST. 2012. "Guide for Conducting Risk Assessments," NIST SP 800-30 Rev.1, NIST, September 2012. http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

66. NIST. 2014. "Framework for Improving Critical Infrastructure Security," Version 1.0, February 12, 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

67. NIST. 2016. "NIST SP 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," NIST SP 800-160, NIST, November 15, 2016. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf.

68. NIST. 2018. "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1, April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

69. NIST. 2018b. "Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems," Draft NIST SP 800-160 Volume 2, March 21, 2018. https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf.

70. NSA. 2018. "NSA/CSS Technical Cyber Threat Framework v1," National Security Agency, March 6, 2018. https://www.iad.gov//iad/library/reports/assets/public/upload/NSA-CSS-Technical-Cyber-Threat-Framework-v1.pdf.

71. ODNI, "Cyber Threat Framework," Office of the Director of National Intelligence. https://www.dni.gov/index.php/cyber-threat-framework.

72. OFR. 2017. "Cybersecurity and Financial Stability: Risks and Resilience," Office of Financial Research,February 15, 2017. https://www.financialresearch.gov/viewpoint-papers/files/OFRvp_17-01_Cybersecurity.pdf.

73. OWASP. 2016. "OWASP Automated Threat Handbook: Web Applications, Version 1.1," November 3, 2016. https://www.owasp.org/images/3/33/Automated-threat-handbook.pdf.

74. Pagliery, J. 2017. "North Korea-linked hackers are attacking banks worldwide," CNN, April 4, 2017. https://www.cnn.com/2017/04/03/world/north-korea-hackers-banks/index.html.

75. Riley, M. 2014. "How Russian Hackers Stole the Nasdaq," Bloomberg Businessweek, July 21, 2014. https://www.bloomberg.com/news/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq.

76. Riley, J.W. 2017. "RSA White Paper: The Shadows of Ghosts - Inside the Response of a Unique Carbanak Intrusion," December 4, 2017. https://www.rsa.com/content/dam/en/white-paper/the-shadows-of-ghosts-carbanak-report.pdf.

77. Roukny, T., Bersini, H., Pirotte, H., Caldarelli, G., and Battiston, S. 2013. "Default Cascades in Complex Networks: Topology and Systemic Risk," Scientific Reports 3, A Nature Journal, September 26, 2013. https://www.nature.com/articles/srep02759.

78. Saydjari, O.S., Stolfo, S.J., and Schutzer, D. 2017. "National Cyber Defense Financial Services Workshop Report: Helping Form a Sound Investment Strategy to Defend against Strategic Attack on Financial Services," BITS, FSTC, and Financial Services Roundtable, Washington, DC, 2010.

79. Schwartz, M.J. 2016. "SWIFT Confirms Repeat Hack Attacks," BankInfoSecurity, April 26, 2016. https://www.bankinfosecurity.com/swift-sees-repeat-hack-attacks-a-9067.

80. Sheingold, P., Bodeau, D., and Graubart, R. 2017. "Cyber Prep 2.0 Draft Instruments for Review: Detailed Questionnaire," PR Case No. 17-2174, The MITRE Corporation, 2017.

81. SIFMA. 2017. "Quantum Dawn IV Fact Sheet," Securities Industry and Financial Markets Assocation. November 9, 2017. https://www.sifma.org/wp-content/uploads/2017/11/QDIV-Fact-Sheet.pdf.

82. Symantec Security Response. 2017. "Attackers target dozens of global banks with new malware," Symantec, February 12, 2017. https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0.

83. Williamson, W. 2015. "Banking Malware Redefined," SecurityWeek, February 18, 2015. https://www.securityweek.com/banking-malware-redefined.

84. World Economic Forum. 2016. "Understanding Systemic Cyber Risk," October 18, 2016. http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf.

85. Woody, C., and Alberts, C. 2014. "Evaluating Security Risks Using Mission Threads," *CrossTalk,* pp. 15-19, September / October 2014.

86. Wueest, C. 2017. "Internet Security Threat Report (ISTR): Financial Threats Review 2017," Symantec, July 18, 2017. https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf.

87. Wynn, J., Whitmore, J., Upton, G., Spriggs, L., McKinnon, D., McInnes, R., Graubart, R., and Clausen, L. 2011. "Threat Assessment and Remediation Analysis (TARA) Methodology

Description, V. 1.0" MTR 110176, PR 11-4982, The MITRE Corporation, October 2011. http://www.mitre.org/sites/default/files/pdf/11_4982.pdf.

88. Zurich Insurance and the Atlantic Council. 2014. "Risk Nexus - Beyond data breaches: global interconnections of cyber risk," April 23, 2014. https://www.files.ethz.ch/isn/182163/Zurich_Cyber_Risk_April_2014.pdf.

ATT&CK™ is a registered trademark of The MITRE Corporation

CAPEC™ is a registered trademark of The MITRE Corporation