Advanced Cyber Risk Management – Threat Modeling & Cyber Wargaming

April 23, 2018

HSSEDI
Homeland Security Systems Engineering & Development Institute

Acknowledgement for DHS Sponsored Tasks

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
This HSSEDI task order is to enable the 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.

Abstract and Key Words

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. This C-Level brief presents HSSEDI's findings and recommendations in its analysis of cybersecurity threat modeling and wargaming for the NGCI program

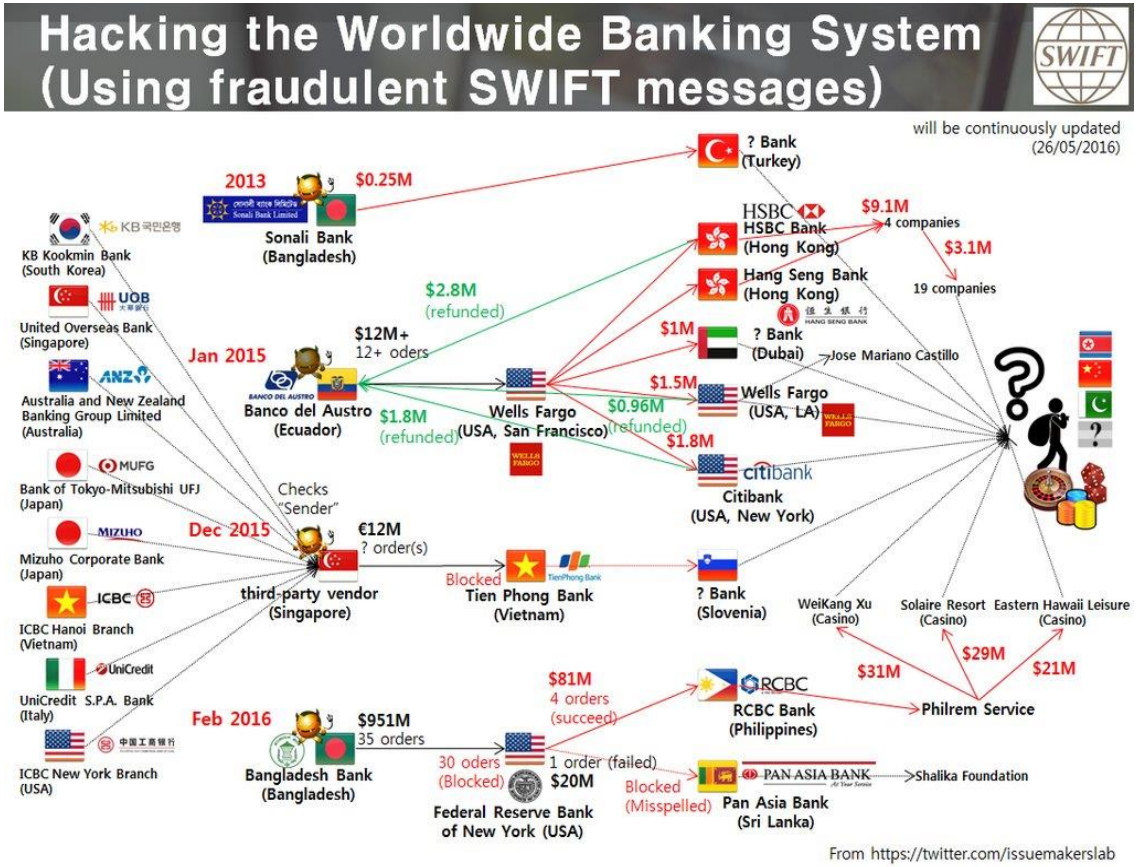
S&T's NGCI Apex program is developing an approach for threat modeling and cyber wargaming that financial services sector (FSS) organizations can use to consider cyber threats and decrease risk. This brief describes a framework for cyber wargaming that balances the strong cyber defense technology focus of detailed hands-on adversarial cyber exercises with the strong business and operational impact focus typical of high-level tabletop exercises focused on cyber. To drive cyber wargaming and assist in managing risk, the brief also describes a framework for an integrated suite of threat models.

Keywords

- Next Generation Cyber Infrastructure (NGCI)
- Cyber Threat Models
- Cyber Risk Metrics
- Cyber Wargaming Scenarios
- Cyber Security; Cybersecurity

Cyber Threat Environment Has Evolved: Not Just Individual But Collective Risks

Modern cyber threats expose institutions to systemic risks through interactions among partner organizations within the Financial Services Sector (FSS)



Recommendation: *Adopt a* **common threat model** *supporting* **enhanced wargaming** *and* **systemic analysis**

HSSEDI
Homeland Security Systems Engineering & Development Institute

Challenge: Reduce Risks to FSS from Cyber Attacks

Cyber defense is too reactive

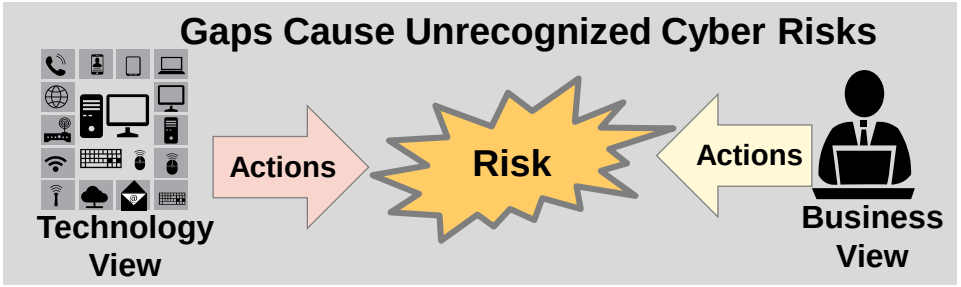
- Anticipate attacks based on business objectives as well as technical characteristics
- Plan and evolve defenses

Cyber risk management has gaps

- Understand interplay of technical and business factors

Sector and systemic cyber risks may go unrecognized

- Link institution-specific frameworks to common threat model for systemic analysis



HSSEDI
Homeland Security Systems Engineering & Development Institute

Solution: Enhanced Wargaming and Systemic Analysis Supported by a Common Threat Model

Communicate across sector via a common cyber threat and risk framework

- Identify systemic cyber risks

Adopt enhanced cyber wargaming connecting business and technical perspectives

- Support with consistent suite of sector-specific cyber threat models

Make cyber risk management more effective

- Reduce cyber risks and gaps
- Reduce cyber breaches and their costs
- Reuse threat analysis and leverage efforts of others in the community

Engage with the NGCI Apex Program's Cyber Apex Review Team (CART) to help achieve this common approach

Effective cyber risk management relies on both business and technical views of attack and impact data

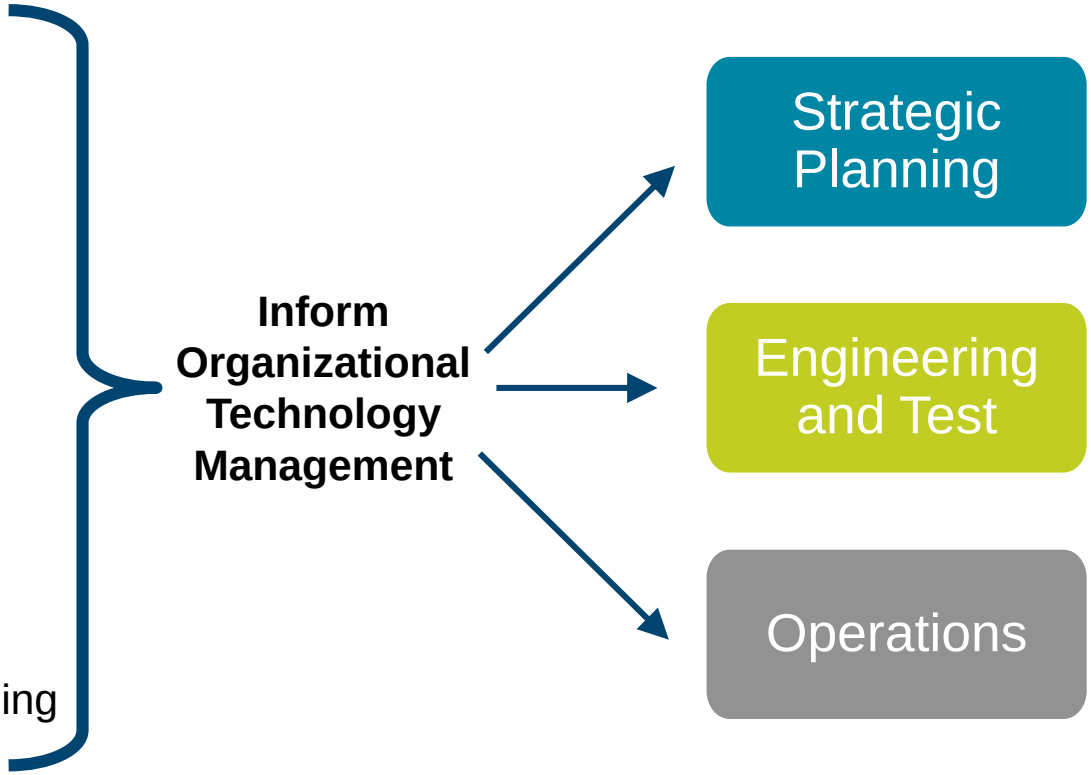
Goals of Cyber Threat Models and Wargames

Cyber threat models capture adversary capabilities and motives

- Anticipate attacker behavior
- Feed cyber wargames

Cyber wargames explore potential scenarios

- Assess and validate defenses
- Uncover gaps
- Exercise procedures and training



Cyber Risk Management Survey

Conducted interviews with 11 FSS critical infrastructure institutions

- Financial institutions, market utilities, and industry organizations
- Executives responsible for cybersecurity threat modeling, risk assessment, and mitigation

Performed cybersecurity literature survey

- 21 threat models and frameworks
- 26 cyber wargaming technologies, platforms, and processes

Drew upon HSSEDI subject matter experts

Findings: Typical FSS Practice

- Organization-specific risk/threat frameworks; most based on NIST[1] and OCC[2] guidance
- Subjective assessment of threats and vulnerabilities; some efforts to quantify consequence
- Documented threat model, but often not comprehensive; subset updated with ongoing intelligence, testing, and events
- One-time product testing against a threat model during acquisition
- Recurring penetration testing
- Tabletop wargaming for coordination and awareness

[1] NIST: National Institute of Standards and Technology
[2] OCC: Office of the Comptroller of the Currency

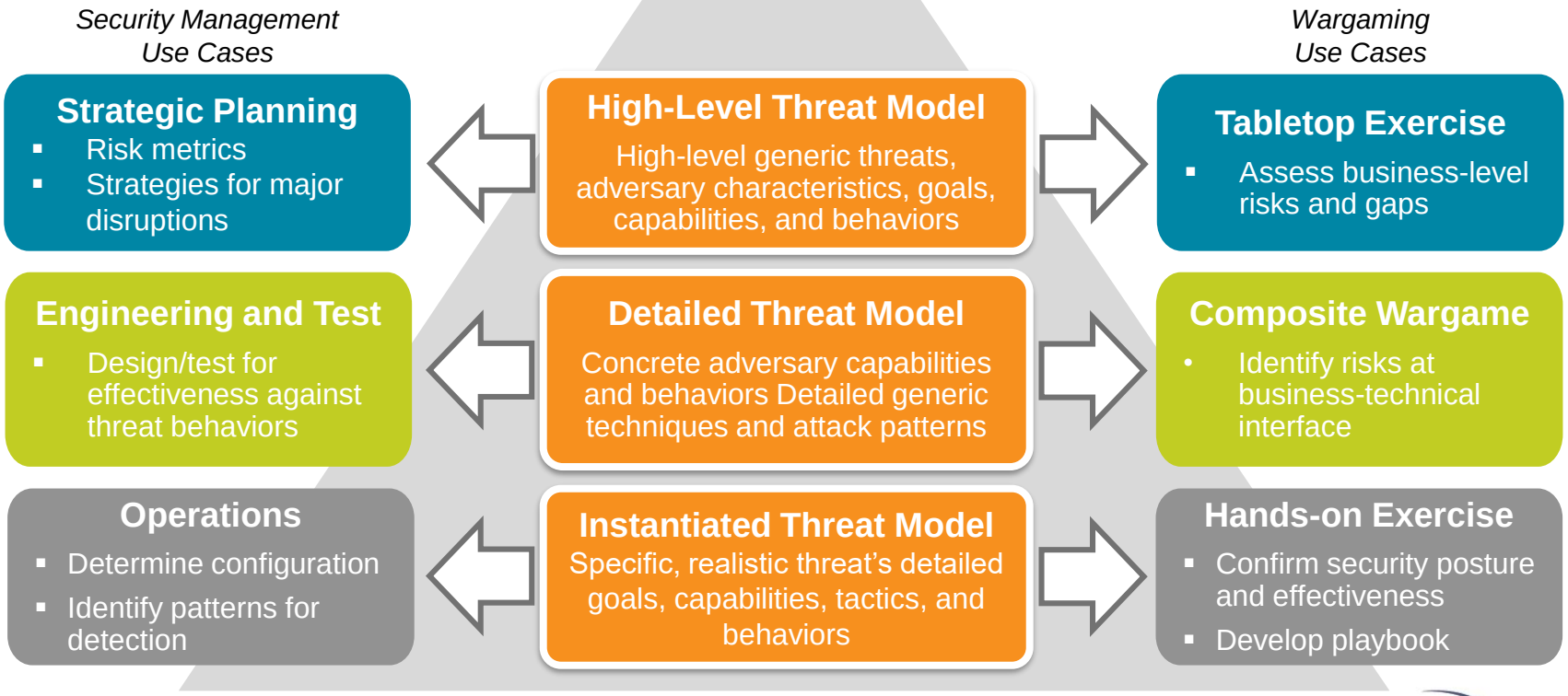
No one model suitable for all uses.*

* HSSEDI, Cyber Threat Modeling: Survey, Assessment, and Representative Framework, 2018.

Use an Integrated Suite of Sector-Specific Threat Models to Support Different Use Cases

Cyber wargames and organizational security management are driven by threat models

- Consistent across levels about the nature of the threat
- Represent adversary's business-focused objectives



HSSEDI
Homeland Security Systems Engineering & Development Institute

Create Composite Wargaming Level to Connect Business & Technical Perspectives

Suite of wargaming levels driven by consistent suite of threat models

Level of Wargame	Participants	Focus	Value
Tabletop Exercises	Executives	Organizational Incident Response	Measure reporting and policy effectiveness
Composite Wargaming	**Mid-level cyber and business managers**	**Test resiliency using goal-oriented scenarios**	**Identify risks from business and technology disconnects**
Hands-on Exercises (e.g., ethical hacking)	Working level cyber staff	Adversary detection capabilities	Measure technology effectiveness

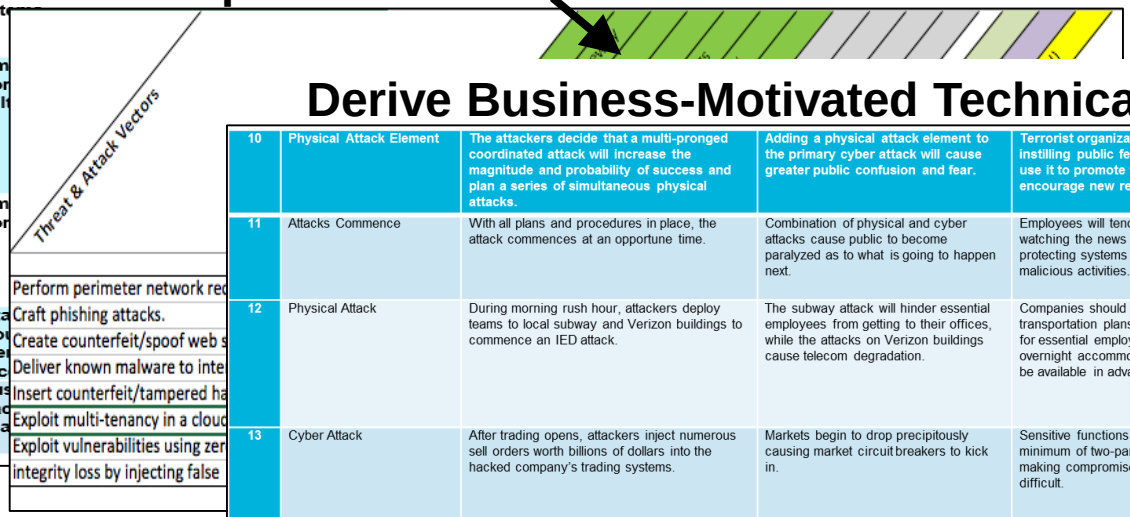
- New composite wargaming level to complement existing methods
- Use to examine interaction of technology, business operations, and shared risks

Use Integrated Cyber Threat Model Suite to Develop Composite Wargaming Scenarios*

Choose Cyber Threat Model Behaviors

Exploit / Control	Compromise information systems or devices used externally and reintroduced into the enterprise.	Mobile or transiently connected devices	Corruption, Modification, or Insertion
Exploit / Control	Compromise softw organizational criti syst		
Exploit / Control	Com infor exfilt		
Exploit / Control	Com infor		
Execute	Obta thro exte Disc		
Execute	Caus attac capa		

Map to Institution's IT Resources and Architecture



Derive Business-Motivated Technical Scenarios

10	Physical Attack Element	The attackers decide that a multi-pronged coordinated attack will increase the magnitude and probability of success and plan a series of simultaneous physical attacks.	Adding a physical attack element to the primary cyber attack will cause greater public confusion and fear.	Terrorist organizations thrive on instilling public fear and strategically use it to promote their agenda and encourage new recruits.
11	Attacks Commence	With all plans and procedures in place, the attack commences at an opportune time.	Combination of physical and cyber attacks cause public to become paralyzed as to what is going to happen next.	Employees will tend to be distracted watching the news and not focusing on protecting systems or spotting other malicious activities.
12	Physical Attack	During morning rush hour, attackers deploy teams to local subway and Verizon buildings to commence an IED attack.	The subway attack will hinder essential employees from getting to their offices, while the attacks on Verizon buildings cause telecom degradation.	Companies should have backup transportation plans available particularly for essential employees. Contingency overnight accommodations should also be available in advance.
13	Cyber Attack	After trading opens, attackers inject numerous sell orders worth billions of dollars into the hacked company's trading systems.	Markets begin to drop precipitously causing market circuit breakers to kick in.	Sensitive functions should require a minimum of two-party authentication, making compromise exponentially more difficult.
14	Attack Diversion	Expecting that other bank employees will notice the irregularities, the attackers also plan to divert attention from the malicious activity by flooding email system with bogus, spoofed messages coming from the new CFO stating that remedial efforts are being taken and that employees should not take any other action for the time being.	Employees do not realize that the emails from the CFO are spoofed and part of the attacker's plan.	Network SPAM filters should be up to date, ready to block malicious emails and not provide employees the opportunity to aid in the attack. Other protective measures include implementing Sandboxes, Email Gateway Inspection and antivirus/host intrusion prevention systems. (See §5.2.1.2 and §5.3.5.1)

* HSSEDI, Cyber Wargaming: Framework for Enhancing Cyber Wargaming with Realistic Business Context, 2018.

Extend to Support Coordinated Cyber Risk Management Across the Sector

Wargaming to extend understanding of:

- Cross-sector risks resulting from risks to individual institutions
- Cross-sector risks from systemic factors

System-of-systems model of interactions and dependencies

Consistent threat frameworks to enable communication/ collaboration

"…there is no common method to quantify cyber risk across firms or sectors, significant time is needed to develop a consensus on a risk measurement standard that would enable financial services to measure and mitigate their individual risk."

- Financial Services Sector Coordinating Council (FSSCC)

HSSEDI
Homeland Security Systems Engineering & Development Institute

Contact for More Information

DHS Science and Technology Directorate

Next Generation Cyber Infrastructure (NGCI) Apex Program

Homeland Security

Science and Technology

Dr. Douglas Maughan (Douglas.Maughan@hq.dhs.gov)
Cyber Security Division (CSD) Director

Greg Wigton (Gregory.Wigton@hq.dhs.gov)
Apex Program Manager