Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security

Research and Development Committee

Research Agenda for the Banking and Finance Sector (Update)

April 24, 2013

Overview

The Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) supports research and development (R&D) initiatives to enhance the Sector's resilience and integrity and to protect both the physical and electronic infrastructure of the Banking and Finance Sector, and its customers.

The FSSCC established the Research and Development Committee (”R&D Committee”) in 2004 as a standing committee to:

1. Identify needs and priorities for research relevant to significantly improving the security and resilience of the Financial Services Sector.
2. Engage the research community (including academic institutions and government agencies) to help them better understand the needs and environmental constraints of the Financial Services community.
3. To identify and help to transition promising research to operational deployment.
4. To coordinate all these activities on behalf of the Banking and Finance Sector.[1]

This research agenda is the R&D Committee's vehicle to communicate the research needs of the Financial Services Sector to the research community. It is envisioned as a “living” document to be updated periodically to reflect changes in the financial services operational environment; the changing threat; and advances in technology.

This document is the third one of the same title. It represents ongoing efforts of the financial industry to ensure that R&D priorities support the objectives of national infrastructure protection plans.[2] This update reflects changes in the FSSCC Threat Matrix, as well as changes in both technology and operational environments. Similar to its predecessors, it incorporates valuable input from the Government, Academic and Industry research community. It describes the Sector's environments, threat, and research needs, and provides guidance in the evaluation and validation of promising R&D. FSSCC support for R&D entails provision of domain expertise to support researchers who profess to be addressing the sector's present and future needs for critical infrastructure protection. Where R&D is deemed by the FSSCC to align with this agenda, the FSSCC may be expected to take an active role in the transfer of such R&D to operational use.

[1] Appendix A provides a list of current R&D Committee members.

[2] Abend, V., et. al., *Cybersecurity for the Banking and Finance Sector*, in *Wiley Handbook of Science and Technology for Homeland Security*, J.G. Voeller, Editor. 2008, John Wiley & Sons, Inc.

Background

Financial institutions have established governance models that include directors of information security, business continuity, and operational risk. These officers manage risk by applying the appropriate mix of technology, processes, and expertise to safeguard people, processes, data, and information systems. Ongoing research and development is vital to supplement these advances, and to securing the economic well-being of the United States.

Thus the focus of the FSSCC R&D Committee is to develop, in partnership with researchers and stakeholders, a mechanism for technology transfer that has clear transition goals, includes intellectual property ownership resolution and metrics to gauge the effectiveness of the R&D solutions in practice. The FSSCC R&D Committee's focus is on providing this transition mechanism.

The R&D Committee has identified four major challenges in relation to these objectives:

1. Greater transparency and communication is needed to make key stakeholders (Financial Services Sector, academia and government) aware of each other's R&D efforts and needs.

2. Better coordination is needed to facilitate activities among stakeholders in the US, as well as coordination with international organizations, subject to legal and regulatory restrictions and national security interests. Better coordination would drive efficiencies, help direct available research investments, and help achieve common goals more effectively.

3. Academics seek access to sensitive data from the Financial Services Sector. However, access to data is a major concern for financial institutions. In general, the Financial Services Sector is reluctant to provide data given the sensitivity of data and the potential for misuse. Better mechanisms for making data available to research but protected against misuse need to be identified.

4. Funding for R&D by the federal government and private sector is inadequate to meet the critical needs of the Banking and Finance Sector. Additional funding is necessary to meet current and emerging challenges.

In response to several of these challenges, in 2007 the FSSCC established a program to connect experts within the Banking and Finance Sector with researchers in academia: the Subject Matter Advisory Response Team (SMART) Program. The program assists research and development organizations working on critical infrastructure protection projects by providing subject matter expertise from financial institutions necessary to facilitate their research and development endeavors. In addition, working with the Treasury, workshops on how the financial services sector operates have been developed and provided to researchers. The program seeks to reduce the gaps listed above by improving mutual awareness between the financial industry and academia, and bringing financial domain expertise to research projects.

This update of the FSSCC R&D Agenda is also directed at reducing the gaps listed above. Previous versions of this Agenda, though clear in their description of Financial Services R&D Priorities, did not provide enough background on the motivation for the priorities. Hence, researchers engaged in work related to the priorities had no criteria with which to define success from a financial industry standpoint. In this version, we clearly outline the state of financial cyber security, and the technology gaps and shortcomings that hinder the industry's efforts to win the cyber war. We map these gaps to specific R&D Focus Areas. Following the description of each focus area is a clear explanation of what constitutes success in technology transfer from research in the area.

Financial Industry Cyber Security Landscape

At a high level the financial industry performs four functions in the National Infrastructure Protection Plan[3].

(1) Deposit and payment systems and products;
(2) Credit and liquidity products;
(3) Investment products including price discovery; and
(4) Risk-transfer products.

This level is useful for categorization of function, but is too high level for specific risk assessment analysis. Systemic functions supporting the operations of the financial sector, such as clearing, settlement, payment and trading, should also be considered critical processes. These systems or processes may be internal to a financial institution or provided by an external party, which may be within the financial sector or may represent other sectors, such as information technology, supply chain management and communications.

A loss or integrity failure in such critical infrastructure could impact the US economy in several ways, including, but not limited to:

- The loss of credit to the market place which includes the creation of new credit or the servicing of existing lines of credit
- The loss of liquidity in the market place which includes the non-availability of funds or assets, inability to move funds or buy/sell securities and commodities to individuals or corporations. Liquidity in this case is in the broadest sense in that it covers all aspects of funds flow.
- The loss of confidence in the operational effectiveness of marketplace which impacts other critical infrastructures.

The Banking and Finance Sector faces a number of trends that challenge the industry's efforts to avoid these losses:

Advances in mobile, social, cloud and other technology advances break down business silos because customers want to be able to transact seamlessly across product lines and channels. These also blur previously well-defined perimeter security models based on obsolete

[3] http://www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf

physical/cyber boundaries, opens up new threat vectors as our systems become perimeter-less, accelerates change, and requires faster decision-making.[4]

Mobile is rapidly growing as the most heavily used component of cyber space, and increasingly physical. It, along with companion cloud applications, introduces new risks and vulnerabilities as well as new tools with the potential for improving our cyber security posture.

The financial industry workplace environment has also changed in a number of ways, including but not limited to:

- Employees bring consumer technology into the workplace—most notably, smart phones and tablets, and the intermixing of personal consumer apps with business functionality[5].
- Both business and consumer data is increasingly available in the cloud.

While these changes could ultimately lead to an increase in the overall security of such information, they currently instead create large stores of important data and processing resources that lure attackers; bypass end point perimeter security;[6] and may evolve to a future infrastructure characterized by a small number of uncoordinated incremental changes.[7]
As the financial industry infrastructure grows more complex, fraud and cyber threats are growing in sophistication.[8] The growing complexity and dependence of our industry on systems that are increasingly real-time increases the risk management challenge.

Threat landscape changes reflect a number of trends in:

- The attackers' motives and objectives
- The attackers' methods and tools
- The attackers' level of sophistication, as well as
- Changes in our cyber environment due to advances in the underlying technology, products, services and applications

Increased experience and professionalism of the cyber criminals, and their access to more sophisticated tools and resources are leading to cyber threat that is increasingly lethal and

[4] See: Gellman, R., *Risks to Privacy and Confidentiality from Cloud Computing*, *World Privacy Forum, http://www.worldprivacyforum.org/*2009, See also: Finneran, M., *State of Mobile Security*. Information Week, 2012(May 2012)

[5] Malware writers have moved from taking a casual interest in mobile platforms to trying to create a viable business model, especially focusing on devices based on the Android operating system. The number of malicious and suspicious apps grew to 175,000 at the end of September 2012, up from 30,000 in June, according to security firm Trend Micro.6

[6] The efficiencies of moving data and applications to the cloud continue to attract consumers, who store their data in DropBox and iCloud, use Gmail and Live mail to handle e-mail, and track their lives using services such as Evernote and Mint.com.

[7] http://www.wired.com/opinion/2012/11/feudal-security/, When It Comes to Security, We're Back to Feudalism, By Bruce Schneier

[8] See: BITS, *Malware Risks and Mitigation*, 2011, The Financial Services Roundtable: www.bitsinfo.org.

successful.[9], [10] Widely published data breach investigation reports make it clear that attacks often succeed in seconds or minutes, but are not detected for days, weeks, months, or even years.[11]

Until this year, the financial sector had primarily been attacked by criminals seeking financial gain, and to a lesser extent theft of intellectual property[12]. This year we have experienced attacks with other motivations[13]:

- Hacktivism leading to disruption and defacing that is politically motivated
- Disruption of Critical Infrastructure by attackers aligned with national agendas and resources

In the near future, it is prudent to also expect attacks with motivations to:

- Control and alter information and on-line profile manipulation to influence what users believe and where they go on the web
- Tamper and manipulate data for disruption of critical infrastructure
- Disrupt and distract the attention of professionals from detecting and defending against coordinated attacks aimed at committing fraud
- Attack equipment through cyber-attacks that could disrupt or take down targeted physical equipment,[14] [15] or take lives[16]

The methods and tools of the attackers have also changed in a number of ways, including:

[9] Operation High Roller, a coordinated cyberattack against 60 different banks, netted hackers some $78 million, http://www.digitalcommunities.com/articles/Special-Report-Cybersecurity-Handbook-for-Cities-and-Counties.html?page=4.

[10] Cyber-Crime 2012: Big Business for Attackers, Big Costs for Victims, by Brian Prince, http://www.eweek.com/security/slideshows/cyber-crime-2012-big-business-for-attackers-big-costs-for-victims/

[11] Bilge, L. and T. Dumitras, *Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World*, in *Conference on Computer and Communications Security*2012, ACM: Raleigh, North Carolina
Baker, W., et al., *Data Breach Investigations Report, http://www.verizonbusiness.com/go/2011dbir*, 2011: Verizon Business (Retrieved 11/1/12).

[12] http://www.wired.com/threatlevel/2012/04/code-not-physical-property/, Code Not Physical Property, Court Rules in Goldman Sachs Espionage Case, By Kim Zetter

[13] DDoS Attacks: PNC Struck Again, http://www.bankinfosecurity.com/ddos-attacks-pnc-struck-again-a-5356/op-1

[14] http://en.wikipedia.org/wiki/Stuxnet, Stuxnet was first discovered in 2010, but in a June 2012 New York times article it was attributed to a US and Israeli intelligence operation, creating an escalation and legitimization of such threats.

[15] http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html, In August 2012 newer variants of Stuxnet were reported

[16] http://blogs.csoonline.com/malwarecybercrime/2479/death-software, Death by software? By bbrenner, Created 2012-12-05 11:03. This article illustrates that as cyber get increasing embedded into our cars, phone, TV's, and even medical devices, death caused by digital disruption through malware is not only possible its plausible, and WatchGuard Technologies suggests that 2013 will be the year a human is killed by a malware attack.

- From relatively static attacks of opportunity, with known signatures, to specific targeted attacks - where attacks are personalized and dedicated to a target
- Persistent attempts at attacking a specified target can last for months and years
- Ability to harness huge resources – botnets and server farms[17]
- Adaptive and dynamic, where the attacker changes approaches, tactics and tools in response to the defense
- Hold unknown vulnerabilities in reserve – large database of zero day exploits created and held in reserve until needed.
- Compromise of the Supply Chain – poisoning components during production and transport. They are hard to detect, expensive to defend against

The financial industry cyber security landscape currently includes a variety of metrics for security decision support.[18] We also employ a variety of cyber defense tactics that can generally be characterized as:

- Shields – Measures that slow down the attacker (e.g. by tactics such as requiring more demanding authentication and limiting authorization), and deflect (e.g. send attacker to special sites that can keep the attacker isolated and possibly also serve as a diversion)
- Blocks – Use of walled gardens (e.g. restrict attacker code to operating in separate containers) and white listing (restrict certain resources and operations to only a validated list of allowed users, including the use of moving target technology that only prior authorized white listed users know how to access).
- Diversions – decoys, false targets and camouflage (e.g. lure attackers to false sites and honeypots that can collect information against them, include false information that only a prior authorized partner can identify as false)
- Actions – intercept and flood attacking sites, create poisoned payloads that the attacker is lured to steal, disrupt sites that are identified as source of attack and intelligence collection

As we move down this list the tactics get more aggressive and will likely necessitate policy-level discussions among leaders and professionals in the public and private sectors.

We have limited resources so it is important to provide business justification for our investments. We need to be able to justify the resources we want to invest in cyber defense, to ensure we are getting sufficient value for our investment. This is particularly difficult to answer when the threat, threat countermeasures and counter-countermeasures constantly change in response to changes in our defenses.

[17] Note that recent DDOS attacks were at as high as 70 Giga bits per second versus earlier attacks more in the range of 10's Giga bits per second.

[18] Bayuk, J., *Security as a Theoretical Attribute Construct.* Computers & Security, Issue TBD, 2013.

Gaps and Shortcomings

Given the currently available technology and the cyber security landscape, the financial services sector faces the following gaps and shortcomings[19] [20]:

1. ***Info Sharing and Analysis*** – Cyber threats ranging from disruption (e.g., DDoS attacks), malware (e.g., account take over), espionage (e.g., intellectual property theft) continue to grow. While there have been significant improvements in information sharing, there is much more that can and should be done. Attacks are not detected early enough in their lifecycle to avoid damage. Forecasting capabilities are practically non-existent. Large segments of the financial community do not have reliable sources for targeted and timely cyber intelligence. Areas needing improvement include earlier detection and better forecasting through improved information exchange between government, private sector security professionals and senior management (C-level)[21], wider dissemination to the entire financial community; and better tactical and strategic analytics[22] , supported by more targeted and timely intelligence[23]. Besides improving our ability to handle crisis events, improved information-sharing and analysis is important to support major policy decisions regarding data collection, data retention, and proactive measures.
    a. ***Achieving the right balance between Privacy and Security*** - The public debate surrounding the information needs for fighting cyber security and the growing concern about preserving the privacy of the individual is likely to intensify. Efforts to strengthen Cyber Security include plans for collecting and retaining

[19] With respect to Cyber Security, the following reports sponsored by BITS - Improving Cyber Security Collaboration Between the Financial Services Sector and US National Security Community, August 2012, Delta Risk; Capability Requirements and Investments for Cyber Security by Financial Services Sector Organizations, January 2013, Delta Risk, identified Information Sharing; Strategic and Tactical Analyses; Crisis Management; R&D and Core Improvement Investment as the key areas needing improvement.

[20] A Joint Associations Cybersecurity Summit was held on January 24 facilitated by the BITS Committee Chair (Kelly King) and The Clearing House Supervisory Board Chair (Richard Davis) that included executives from key financial sector associations and the U.S. Treasury Department to discuss the rapidly expanding cyber risks, its growing and potentially systemic impact on the sector, and current and future activities necessary to address the challenge; and to develop a comprehensive cyber roadmap, with 24 activities to enhance information sharing, and improve strategic and tactical analytics, crisis management, core component of the cyber eco-system through R&D, and executive communication and advocacy.

[21] More effective C-suite communications is needed for better management of external communications during crisis and to support decision processes with respect to appropriate responses and courses of action, including when to move to more active defenses.

[22] This includes the need for increased automation assistance to enable processing of greater volumes of data, support on-demand threat information availability, and provide the capability to assimilating multiple threat data to better identify threat activity and produce threat profile identification

[23] This necessitates an increase in the number of industry personnel with security clearances, and a faster more efficient clearance process

more data, yet there is a growing concern about preserving the privacy of the individual that could result in policy that can inhibit or restrict the collection and use of much of this data. Our industry needs to partner with policymakers and privacy advocates to better define which activities are socially acceptable, to assess the value of data uses against potential privacy risks, and to examine the practicability of obtaining true and informed consent and enforcing restrictions on data flows. These findings need to be translated into a better understanding and articulation of the most fundamental concepts of privacy law, taking into account societies needs for better cyber security.

   b. ***Cyber war and Active/Passive defense* –** There is a whole spectrum of measures and countermeasures that we can take to defend against a cyber-attack. Some measures can be taken before the actual attack, at the planning and reconnaissance stage, others during and after the attack. The actions can range from purely defensive, such as turning off all non-essential services, to proactive measures[24]. We need to be able to accurately assess the situation, understand the effectiveness of the various actions that can be taken for the situation at hand and the circumstances where various actions taken across the spectrum of potential adversary disturbances can be justified under existing laws and policies.

2. ***Define cyber risk readiness*–** Based on proposed legislation and the recently issued Executive Order[25], the Government is seeking higher standards and practices along with requirements for increased reporting and auditing for cyber security readiness and resilience. However, existing standards have been shown to be inadequate [26] and no source for improved standards has been proposed. There is no consensus among experts on what cyber risk readiness entails. The financial services sector needs to be able to better understand and articulate what the right level of cyber readiness is, and how it is best measured and assessed, and what are the associated liabilities.
3. ***Cyber security education and awareness* –** Better cyber security is everyone's job, our employees, business units and our customers. Cyber security is not just a technical problem, it is a people and process problem, and it cannot be left solely to the cyber security professional. Though we have tried to train users, operators and stakeholders of financial services on cyber security practices, both the practices, and the desired behavioral outcome are inadequate to the challenge of thwarting known threats. We need to learn how to do a better job of educating, raising cyber security awareness and motivating people to practice good cyber health.

[24] What active defensive measures could be taken, under what circumstances and by whom, is an area of much discussion and analysis, including the relative roles of Government, DoD and financial services sector. Although most of this falls into the area of policy and legislation, research in areas such as improving attribution can help.

[25]Executive Order -- Improving Critical Infrastructure Cybersecurity, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, Presidential Policy Directive -- Critical Infrastructure Security and Resilience, http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[26] See: Mogull, R., *An Open Letter to Robert Carr, CEO of Heartland Payment Systems*, in *Securosis Blog*2009, Securosis.

4. ***Dependency on other Critical Industries*** - Our sector is dependent upon the cyber-resiliency and cooperation of other critical industries, such as telecommunications, information technology, power, and transportation sectors. We need to better understand these inter-dependencies so we are not taken by surprise by them.
5. ***Secure architecture, processes and testing*** –Many aspects of our systems architecture, software, and processes are inherently unsecure and are not suited to the purpose of controlling financial transactions. . We need to figure out a way we can more easily and quickly migrate to new, more secure architectures, processes and testing practices. We are still struggling with how to move many of our legacy core processing systems that are more than 20-30 years old, to more cost-effective, agile, integrated systems. Moving from existing architectures and processes to new more secure ones will be at least as difficult. The new more secure architecture, process and testing must include consideration of the move to Mobile and the Cloud, and the need to improve existing Identity and Authentication technology and processes.
6. ***R&D focus*** - Cyber security is not a static activity. Like war, we are faced off against an intelligent, agile adversary who is constantly learning, improving and adapting to our defenses. We need to be equally adaptive and resourceful. We need a focused cross discipline (technology, sociology, political, legal and economic) R&D program that can address the needs articulated above so we can not only continuously assess and improve how well we are performing, but continue to invent new “game-changing” defense strategies, tactics and technologies.

We have updated the FSSCC Research Agenda to address the above gaps and shortcomings discussed above.

Research Agenda for the Banking and Finance Sector

Based upon the Gaps and Shortcomings identified, we have proposed a set of 10 R&D focus areas. Table 1 maps the R&D Focus areas to the Gaps and Shortcoming they address. The discussion of the R&D Focus areas below discuss how they address the identified gaps and shortcomings; examples of research areas they include; criteria for success and desired outcomes, including likely impact on our organization and processes.

TABLE 1 – Mapping of R&D Focus Areas to Gaps and Shortcomings

← Gaps and Shortcomings __ →

R&D Focus Areas	**Info-sharing and Analysis**	**Defining Cyber Risk Readiness**	**Cyber Security Education and Awareness**	**Dependency on other critical industries**	**Secure architecture, process and testing**	**R&D Focus**
1. Identity	**X**	**X**			**X**	**X**
2. Analysis and Intelligence	**X**	**X**		**X**		**X**
3. Transaction protocols					**X**	**X**
4. Risk Mgmt	**X**	**X**				**X**

5. **Human Behavior**	**X**		**X**		**X**	**X**
6. **Proactive Measures**		**X**			**X**	**X**
7. **Technology Assurance**		**X**		**X**	**X**	**X**
8. **Testing**	**X**	**X**			**X**	**X**
9. **Training**		**X**	**X**		**X**	**X**
10. **Architecture/ Infrastructure**				**X**	**X**	**X**

1. Identity Assurance

Fundamental to almost any security and fraud defense is an improved ability to better identify and verify who we are communicating and exchanging information with, and who we grant various rights and entitlements to. This not only includes people and organizations, it also includes the hardware, software, and application services we use and depend upon. Higher assurance identity and authentication of people, services, devices and software is a necessary component of any solution that successfully addresses the gaps and shortcomings identified in information-sharing, readiness, architecture, process and testing. Strengthening mutual customer and financial institution identification and authentication can make it much more difficult for an attack to succeed and can improve trust in the financial institution brand and provide a platform for trusted information vault services.

Our current Identity assurance processes strength is eroding at a number of levels. It is becoming increasingly difficult to correctly and uniquely identify[27] a new customer at enrollment/on-boarding with the level of assurance commensurate with the risk.

The process of authentication occurs for us is when a customer claims the identity setup for them by providing proofs (credentials and/or authenticators”) of that identity. This most often happens when the customer attempts to access their accounts in order to take actions such as making payments and paying bills. It is also becoming increasingly difficult to authenticate an individual with a high degree of confidence. The current crop of credentials have become increasingly vulnerable to copying, counterfeiting and spoofing. This is further aggravated by the increasing

[27] This can include their relations with others

number of credentials needed by a customer to access their many applications and services, leading to practices that increase the vulnerability of the authentication process[28].

Once the user is authenticated, a completely separate process, authorization, takes over as the user receives the entitlements they have been assigned. Although these are independent processes they can impact each other. Low confidence in an authentication may require real-time verification of an attribute to increase confidence; requests for authorization of high risk transactions may require additional levels of authentication and/or identity attribute verification; and fine-grained authorization (such as selective delegation) needs to be supported with equally fine-grained authentication (ability to reliably distinguish between a primary account holder and an individual or employee delegated only certain rights and privileges)[29].

The erosion in the identification and authentication processes is occurring for several reasons, including:

- Loss of our ability to use “password” as the single trusted user identity authentication token. This is due to the increasing sophistication of techniques to compare or steal passwords.
- Compromises of trust roots such as OTP (one-time-password) seed servers and root Certificate Authorities (CAs), and the growing ability of techniques to compromise or steal authentication tokens. [30]
- Compromises of hashed, encrypted, and clear text password databases
- Increasingly comprehensive rainbow tables[31]
- Increasingly sophisticated and targeted social engineering attacks on passwords and answers to Knowledge-Based Authentication (KBA) questions
- Loss of our ability to use other secret “things you know”, such as hint questions. This is largely due to the increasing access to public-records sources of answers to KBA questions and access to an individual’s personal information via social networking sites.
- Advances in technology and criminal sophistication make it easier to forge credentials and manufacture synthetic identities, compromising Identity Proofing processes.
- Inadequate verification of the identity of a web service, device or software application[32]

[28] A contributing factor is the unmanageable number of passwords people must remember to access their online accounts. Many people don't even try; they just re-use the same ones for all of their accounts, making it that much easier for identity thieves., http://www.nist.gov/nstic/

[29] Absent this capability for fine-grained authorization, users often resort to sharing their credentials (e.g. passwords), often leading to additional vulnerabilities.

[30] See Federal Financial Institutions Examination Council, “Supplement to Authentication in an Internet Banking Environment”, June 22, 2011

[31] http://en.wikipedia.org/wiki/Rainbow_table, A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes.

[32] This need becomes increasingly important as we evolve to an Internet of Things (IoT). Lack of adequate verification of the identity of a web service or application also provides opportunities for social engineering and

- Inadequate ways to alert and warn consumers and motivate them to act more securely, such as not clicking on an untrustworthy link or providing sensitive information to a suspect or unverified website.

We need a better technology and a plan to vastly improve our ability to identify and authenticate people, software and systems in a way that is more resistant to spoofing and compromise. This includes trust models and legal and policy frameworks.

Research areas include (but are not limited to):
(a) Establishing confidence in identities of persons, corporations and other entities, at the time of userid creation or service enrollment, including collection of information which will assist in strong identity verification in future interactions, and in the re-establishment of lost or stolen credentials.
(b) Establishing confidence in verifying/authenticating identities of persons in ways which do not rely on secrets alone. This would include things you have, such as tokens, things you are such as biometric identification, behavioral and transaction analysis. Other methods, which raise the bar on technical (e.g. man-in-the-browser) and social engineering attacks, would include increased use of encryption technologies, but in ways that are acceptable and easily comprehended by the users.[33]
(c) Methods of establishing confidence in identities of persons in ways which do not require rooted trust (again, see b).
(d) Establishing confidence in verifying/authenticating things (e.g. services, applications and devices)
(e) Need for better ways to measure and communicate the assurance associated with identity verification and authentication services to enable or allow the sharing or interchange of identity information between financial and other institutions.
(f) Need for identity systems designed to be resistant to identity spoofing
(g) Need to study and pilot identity and authentication solutions with regard to for their usability and acceptability. Any solution should be easy-to-use with sufficient value-add to the user (e.g. minimal invasiveness, operating transparently and securely, and in a manner that is privacy-enhancing) and cost-effective (compelling ROI) to ensure its successful take-up so that user acceptance is high.

Criteria for success and desired outcomes:

People, organizations, devices, services, application software and their attributes and entitlements are authenticated in real-time at the level of assurance commensurate with the risk. This means that the credentials or authentication tokens asked of the customer and the authentication layers employed get escalated as the associated risk of the information being accessed increases and the threat environment increases, yet remains easy enough to use that user

theft of personal identifying information and passwords and other authentication credentials through web service and application spoofing.

[33] An example of a good use of technology, albeit in the password space, is the use of pins instead signatures for credit card transactions in Europe and its increasing use in the U.S.

acceptance is high. These identity layers will have to work in the presence of and co-habitation with untrusted consumer devices and networks

One criterion of success would be a dramatic (order of magnitude) reduction in successful identity impersonations, synthetic identities, and false positives and negative authentications and authorization due to both error and spoofing attacks.

2. Security Analysis and Intelligence

The description of gaps in information sharing and analysis makes it obvious that the financial industry needs faster and more effective tools for detection and intelligence collection of security anomalies, attacks (including zero day attacks), and incidents. Security operations teams need increased automation to enable processing of greater volumes of data, support on-demand threat information availability, and provide the capability to assimilate multiple sources of threat data to better identify threat activity and produce threat profile identification.

There is no expectation that the type of data collected by current intrusion detection tools or existing attack repositories is directly applicable to the types of problems expected to be faced by security operations teams in the near future. Hence, a premium must be placed on the ability to customize both data gathering tools and data models. Today’s signature-based models are expected to be replaced by attack sequence models wherein data sources vary both in format and extraction protocols. Where signatures are preserved, they are expected to expand into flexible hash techniques that omit irrelevant noise and instead focus on attack pattern matching.

Security metrics of various types (target, process, activity) should also be employed to quickly assess the technology environment in order to determine the impact to system configuration of a known attack in progress. This involves blending what we today consider cyber forensics techniques with real-time monitoring capabilities. Security health-checks should be automated in order to allow for instant verification of continued functionality of security controls such as network filters and audit trails. Redundant and diverse monitoring techniques should support real-time analysis of incidents in progress. The data collected in the course of such analysis should be useful not just for operational decision support, but also for security design decision support. Such data is also expected to be used in tools for trend analysis and threat modeling.

Visual displays of quantitative information and cyberspace architecture should be developed that facilitate our ability to analyze and understand current threats while boosting our ability to forecast future adversary capabilities so that the industry can anticipate “where the puck is going to be.”[34] Such tools should allow us to better understand our vulnerabilities; this includes understanding the complex interdependencies (logical, physical, temporal and psychological) of our systems at least as well as our adversary – Potential research areas on this front include the identification of security metrics appropriate for forecasting anomalies in adversary behavior,

[34] http://www.brainyquote.com/quotes/authors/w/wayne_gretzky.html, “I skate to where the puck is going to be, not where it has been” Wayne Gretzky

detecting insider threat, and conducting cascade analysis; that is, investigation into how a vulnerability exploit in one or more systems may be expected to impact other systems and/or grow in severity.

.

Even the most straightforward cyber security analysis requires platforms that can store massive amounts of both structured and unstructured data, and automatically identify correlations. Such automated correlation techniques must be transparent to security analysts in order for them to benefit from advances in this technology. Security incident workflows must be developed to enhance security analyst effectiveness via both inter-firm and federated data collection and sharing models. These may include triggers for automated forensic and fraud data collection from multiple financial institutions and real-time generation of sector-wide historical trend analysis. Such data must be produced in a manner that allows for immediate information sharing in a structured but flexible format.

Research areas include, but are not limited to, tools and methods that support:
(a) Real-time or near-real-time detection of anomalies which might indicate an attack or vulnerability.
(b) Forensic analysis of attacks in real time or near real time.
(c) Reducing noise and false positives in security event management systems.
(d) Real-time or near-real-time visualization of system state, event traffic, and user and adversary behavior to facilitate human detection of anomalous and malicious behavior.
(e) Rapid identification of system weaknesses exploited by newly discovered attacks.
(f) Techniques for discovering and collecting intelligence on new exploits before they get deployed
(g)Models for anticipating/forecasting new threats that are supported with realistic-to-gather data repositories.
(h) Database schemas and repositories that support globally distributed cyber security data collection and near-real-time analysis
(i) Application instrumentation to produce transaction-specific audit trails that include details of corresponding infrastructure
(j) Software security metrics that can be used for quick and accurate malware identification
(k) Identification of security weather metrics, or observable indicators or changing adversary behavior.
(l) Identification of internal firm activity metrics to identify behavioral trends which correlate with security incidents.
(m) Methods of sharing actionable security metrics and indicators of compromise, without compromising privacy (such as anonymizing data), to allow for industry-wide analysis.
(n) Visualization tools which support exploration of large corpora of event and log data with the objective of identifying entirely new types of threats, risks, and attacks

Note that advances in item (m) may only be useful when combined with an increase in the number of financial industry personnel with government security clearances, as a great deal of actionable intelligence in the cyber security realm originates from classified operations. Methods of facilitating information classification, segregation, and targeted distribution according to information sharing policies and privacy are thus within the scope of the agenda item, as well as methods to increase the efficiency of the private sector cyber security worker clearance process.

Criteria for success and desired outcomes:

Security analysis and intelligence should be approached as if the systems in scope of a cyber security analyst’s responsibility were part of a large manufacturing line with rigorous requirements for each element to be exactly measured and monitored for conformance, facilitated with state-of-the-art scientific instrumentation. Research contributions in any one area should be demonstrated to have utility in achieving the target vision. Pathways to technology transfer should be intuitively obvious when the research is considered as a means of improving a security analyst’s ability to understand, predict, and protect system operation in the face of changing threats.

Deliverables, within the scope of this success criterion, include built-in sensors and tags in all critical systems and devices can be integrated with massive sources of structured and unstructured data[35] to enable real-time identification of malware, infected devices, and suspicious activities of people and organizations. These analyses are capable of learning and adapting to changing threats and tactics through feedback from real-time and after-the-fact forensic analyses. The result would be a dramatic decrease in the effectiveness of current and projected attacks. The likelihood of an attack succeeding from planning to successful execution is reduced to less than 1%, and of an attack succeeding a second time close to zero.

3. **Transaction protocols**

We need to upgrade and/or redesign our underlying technology infrastructure and processes to be more resistant and resilient against cyber-attack. In particular, current financial technologies and transaction protocols exhibit weaknesses which create opportunities for exploitation by adversaries; for example, credit cards present clear text copies of information (card number, CVV code) which is treated as secret authentication data in transaction protocols. Many transaction systems such as web banking can be overwhelmed by advanced DDOS attacks. Better physical artifacts and transaction protocols are required to guard against fraud and to improve resiliency, ensuring that sensitive data.is not leaked or tampered with, that fraudulent and unauthorized transactions are detected, and a system is resilient against service denial attacks.

Research areas include (but are not limited to):
(a) Protocols involving additional parties to improve security, and that compensate for vulnerabilities in the underlying information and communication technology (ICT) infrastructure and protocols they are built on top of.
(b) Real-time or near-real-time closed-loop protocols to decrease the time between commission and detection (by end users or institutions) of fraudulent transactions.
(c) Zero-knowledge proof and related protocols to reduce exposure of secrets to merchants and processors.

[35] Big Data and Big Data analyses

(d) Improved consumer devices which decrease the value to adversaries of a stolen device.
(e) Improved point-of-sale devices which decrease the likelihood of merchant fraud.
(f) Protocols with enhanced accountability features which make it easier to identify perpetrators of fraud.
(g) Protocols and devices which are resilient in the face of compromise of root keys or of cryptographic or hash algorithms, or tampering of information
(h) More robust real-time processing protocols, architectures, processes and tactics
(k) New, innovative and more effective defense technologies, strategies, tactics and processes
(l) Architecture designs and processes that complement these protocols to collectively present both a impenetrable barrier against unauthenticated people, devices and software and a moving target with respect to access by any non-verified person, software or device, even in the face of counterfeit or tampered credentials. These protections need to be built in a manner that is transparent and easy to use and design new applications for by verified entities, but difficult or near-impossible by non-verified entities.
(m) Protocols which support rapid, non-disruptive replacement of cryptographic and hash algorithms, to support quick industry-wide recovery from breaches of cryptographic primitives.

All such protocols should be cognizant of the needs for security analysis and intelligence and integrate real-time audit trail capability that is easy to integrate into security information management systems.

Criteria for success and desired outcomes: A core transaction protocol layer, integrated with transaction systems and processes, that is easy to use and customize by verified users and devices, but near impossible to access, modify and tamper with by any non-verified user or device, where the associated verification process and transaction protocols can change and adjust based upon the changing threat and available resources (input from security and threat analysis). These designs must be able to require an exploitation work factor of more than a thousand times the computational resources required by a valid user or system. They must be able to handle loads of hundreds of millions of financial transactions per day.

4. Risk Management

We are using the wrong math to manage operational and security risks. Probability theory accurately predicts losses arising from random processes; intelligent adversaries are not random processes. We are using the math developed for blackjack to estimate our chances at three-card Monte.

We need better methods for analyzing security risks, and relating them to other risks (e.g. operational, credit and market risks) with respect to aggregating them to understand total risk exposure to all the various risk types (“windows”) against common metrics, better understand the effectiveness of various risk mitigation solutions with respect to their effectiveness over time, and being able to trade off the risk mitigation costs to the residual risk. Additionally:

- To date we have had very limited success in modeling and predicting the risk of cyber security attacks in any measurable way.

- It is harder to make investment decisions for cyber as we cannot always quantify the cost of a cyber-risk as easily as we can in the case of market and credit risks. Or even make relative comparisons between different cyber threats.
- Operational risk, market and credit risk are often evaluated as if they are three independent risks, they are inter-related and models need to be developed that include these inter-dependencies[36].

Research areas include (but are not limited to):
(a) Game theoretic methods for analyzing exposure to security losses
(b) Monte Carlo tools for analyzing future consequences of present actions
(c) Bayesian inference to incorporate additional knowledge and evidence as learned
(d) Scenario analysis to analyze possible future unexpected events and outcomes
(e) More effective tools for exercising and evaluating our risk management processes
(f) Ways to manage and trade-off low likelihood, high impact risk situations (e.g. black swans and perfect storms)

We note that many of these tools discussed in the research areas exist in the context of statistical analysis, but they are not customized for financial sector or cyber security scenarios, and research published on security topics using these tools typically contain unsupported assumptions that security decision-makers have reliable ways to gather and represent data. In order for these tools to be effective in supporting the financial industry critical infrastructure protection requirements, they must consider the operational context in which cyber-security and fraud decisions must be made in real or near-real time.

Criteria for success and desired outcomes: A common framework and set of metrics and processes are developed against which cyber risk can be identified, assessed and managed against other financial risks such as credit and market risk. This includes an improved understanding of the impact of various risk mitigation decisions across all the dimensions of risk (such as credit, market, operational, legal) that the individual financial enterprise and sector must manage against. It also includes the ability to continuously track, measure, and improve the effectiveness of the various risk mitigation and response management measures and processes.

5. Human Behavior

Problem

[36] For example, market risk is associated with the loss experienced due to market price fluctuations, such as economic downturns. Credit risk is associated with the loss due to credit defaults and the likelihood of occurrence of credit defaults is often increased in a market downturn where there is a tightening of credit and an increased occurrence of loan defaults. Similarly an increase in operational risk, either brought upon by a sudden increase in natural or man-made disasters or a disruptive cyber event, can bring about economic downturns in the market and loan defaults. This need for an integrated model of market and credit risk has been recognized, and models have been proposed, but work remains to build an integrated model of market, credit and operational risk.

Human behavior has long been a cause for the significant increase of risk. For even the most hardened, well-secured organizations, human behavior is a major concern. Whether through acts of commission or omission, human behavior has been the root cause of many high profile breaches. As technology has become more intricate and advanced, social engineering, insider fraud and corporate espionage have become the tools of choice for the would-be intruder. The topic of Human Behavior includes four primary categories for future research: Motivation, Commission, Omission and Integration.

Research areas include (but are not limited to):

Motivational

This area includes all areas of thought that are often difficult to describe but typically lead to either acts of commission or omission.

(a) Determine whether motivation is a solid leading indicator for the purpose of determining the probability of adverse human behavior (Commission and/or Omission).
(b) Determine the actual effects/probable outcomes of different motivators.
(c) Analysis of the human motivation behind the desire to commit an act of commission.
(d) Analysis of the motivation/environmental issues that lead to acts of omission.
(e) Understand the process that motivates an employee, vendor, partner or outsider to engage in an act of commission/omission.
(f) Research and understand the motivation to adhere to security controls and/or improve the security of a system.

Acts of Commission

These acts are best described as the illegal acts taken by an employee, vendor or outsider in which to gain access, steal data, harm an organization, and all other repercussions of a security related incident. The following are listed as primary areas of research:

(a) Research and describe typical behavior prior to negative act of commission
(b) Research and description of typical behavioral cues following negative act of commission
(c) Analysis of the common traits of those who display atypical behavior (sociopathic tendencies) and will not exhibit consistent behavioral norms.
(d) Analysis of the legal issues surrounding the monitoring and profiling of employee behavior to determine the probability of acts of commission.
(e) Analysis of the impact on privacy of employees in an organization that monitors and profiles human behavior.
(f) Analysis/Discussion regarding the morality & effectiveness of using preemptive notification regarding those who display behavior outside individual control areas
(g) Analysis of the effective implementation of pre-employment controls, such as background investigations, as a leading indicator

Acts of Omission

These acts are typically unintended. Employees, vendors and trusted partners may exhibit behavior or engage in actions that open an organization to the negative consequences of a security breach.

The following are the areas of potential research:

(a) Analysis of human cognitive biases and limitations and how these can be exploited to encourage and reward secure behavior.
(b) Analysis of how adversaries exploit human emotions, beliefs, and cognitive biases to defeat secure systems and perpetrate fraud.
(c) Analysis of cognitive cues which can create a feeling of risk or danger in humans who are engaging in insecure or malicious behavior.
(d) Research and document the required actions in which to transition effective security awareness and training into real world implementation to effect positive behavioral change.
(e) What actions taken by system designers, engineers and developers inherently lead to acts of omission?
(f) When does an act of omission become an act of commission?
(g) Are there typical behaviors associated with covering up a negative act

Integration

Once the motivation, acts of omission and acts of commission are fully researched and documented, the program must determine the best path forward in which to integrate the information into the organization; this includes:

(a) From the outset, the integration of behavioral indicators with the overall risk management program is key. Research the best cases in which to implement this integration.
(b) Research the effective implementation of behavioral indicators with technical and non-technical security controls.
(c) Create a mapping/matrix of behavioral indicators with appropriate/effective security controls.
(d) Research the utilization of security tools to baseline, monitor and alert on behavioral issues
(e) Research and recommend the implementation of incident handling/reporting as it regards behavioral issues. (This is important so as to not escalate minute negative issues.)
(f) Implement a positive feedback loop for the continual improvement of the system.
(g) Develop a quantitative manner in which to determine the effectiveness of the program.

Other more general behavioral research areas include (but are not limited to):
(a) Analyses of human motivations to behave securely or insecurely relative to using financial applications
(b) Analyses of human cognitive biases and limitations and how these can be exploited to encourage and reward secure behavior.
(c) Analyses of how adversaries exploit human emotions, beliefs, and cognitive biases to defeat secure systems and perpetrate frauds; perhaps even build a test set that can be used to validate proposed solutions

(d) Research on WHAT it takes in the area of awareness and training to ACTUALLY effect behavioral change.

All of these research areas should be able to justify their definition of secure behavior in an operational context, and should not make assumptions that any measureable aspects of such behavior as yet exist. Moreover, our industry needs to partner with policymakers and privacy advocates to better define which activities are socially acceptable, to assess the value of data uses against potential privacy risks, and to examine the practicability of obtaining true and informed consent and enforcing restrictions on data flows.

Criteria for success and desired outcomes: There are several dimensions of such criteria with respect to research in human behavior. Motivational, commission, and omission research is helpful, but unless these are combined with risk management techniques, success criteria will not be met. More detail on these dimensions follow.

Motivational

(a) Create a motivational criteria and the associated typical outcomes
(b) Create a list of top behavioral indicators for security compliance

Commission

(a) Create a listing of behavioral cues that lead to the act of commission
(b) Create a listing of behaviors that occur during an act of commission
(c) Create a listing of typical behaviors that follow an act of commission
(d) Legal, privacy and morality documentation regarding behavioral monitoring
(e) Provide a list of pre-employment recommendations in which to deter or remove the possibility of an act of commission

Omission

(a) Documented case studies and findings as to how adversaries exploit human behavior
(b) Listing of cognitive cues that create a feeling of risk
(c) Determination/documentation as to when an act of omission becomes an act of commission
(d) Create a listing of behaviors associated with the covering up of an act of omission
(e) Create a listing of programmatic functions that lead to acts of omission

Integration

The integration of human behavior into risk management, information security and physical security programs is aided by a system development and operational life cycle management guide that includes:

(a) Human behavioral integration model for risk management and information security
(b) Vendor agnostic mapping of technical security controls as they relate to behavioral indicators
(c) Incident handling methodology, both preemptive and reactive, for dealing with human behavior related issues
(d) Training required to ensure the integration of the human behavior model throughout the organization
(e) All associated policies/procedures and non-technical security controls recommended for a successful program

The guide includes quantitative criteria to determine the effectiveness of the implemented integrated program

6. Proactive Measures

The financial services sector is fighting an asymmetric battle against its adversaries; we create static defenses against every possible attack, while adversaries create targeted attacks on only the weakest points of our systems. In light of this, we need better defensive tools, tactics, and processes that enable us to respond with more agility. Not only do our defensive tools need to be more effective, but we need to be able to apply a variety of alternative responses and adaptively change them in response to the attackers changing techniques and tactics. We need to develop methods which can be tailored to actively disrupt adversary activities, impose significant costs on attackers that reduce their incentive to attack, and require them to divert resources from attacking our systems. These measures must be able to rapidly adapt to changes in adversary capabilities and tactics.

Research areas include (but are not limited to):
(a) Methods of disrupting attack tools
(b) Methods of imposing heavy economic costs on attackers
(c) Methods of increasing the chance that an attack can be traced back to its originator in a way that is supported by evidence admissible in court
(d) Methods of inducing attackers to waste resources attacking dummy targets
(e) Techniques to enable more effective C-suite communications needed for better management of external communications during crisis and to support decision processes with respect to appropriate responses and courses of action, including when to move to more proactive responses.

Criteria for success and desired outcomes: A suite of proactive measures should be developed that provides demonstrative success over current purely defensive measures, including a set of tools and analyses that justifies countermeasures and a confidence level, based on the projection of potential damage if these measures are not taken, a knowledge of the perpetrators, their methods and motivations. These measures need to take into account the unique regulatory and compliance environment of the financial services sector.

.

7. Software Technology Assurance

The vast majority of successful attacks on software systems exploit a small number of known types of vulnerabilities (SQL injection, cross-site scripting, buffer overflows, session management weaknesses, etc...); these vulnerabilities are cataloged in the OWASP Top 10 Application Security Risks list. Better tools are needed to eliminate as many of these issues as possible from new and existing applications.

We also need to improve how we architect our systems so we can identify and verify hardware and software, and that this “trusted” hardware and software can operate more securely even in the presence of malware or tampered code. We need to be able to trust the hardware, software and application services we use and depend upon to operate reliably and to only perform those things they were designed to perform and nothing else. We need to be able to build on top of a core that is not vulnerable to exploitation, and can detect and report if they have been tampered with, or contain hidden malware and spyware.

Research areas include (but are not limited to):
(a) Methods for decreasing the false-positive rates of dynamic analysis tools
(b) Tools for imposing strong type-checking and input validation on the data submitted to existing applications
(c) Languages, compilers, and analysis tools designed to eliminate OWASP top-ten vulnerabilities
(d) Research on what it takes to train and motivate developers in a way that it affects what they do and how they do it
(e) Ways to build in end-to-end SDLC with security features so they have a better chance of being used
(f) Ways to architect and code software so it is more resistant to unknown vulnerabilities and future attacks, and more resilient when under attack and/or in the presence of malware and untrusted processes.
(g) Ways to architect and code software so they can mimic some of the defense measures of biological systems, where future attacks can be isolated, analyzed and defenses and measures developed and implemented in real-time.
(h) Ways to verify the authenticity and integrity of web services, devices and software applications, including the ability to trace its history from its original production through the sequences of its formal ownership, custody, and places of storage and modification, linked to authenticated persons, corporations and other entities.
(i) Methods by which software may be resilient against both hardware and software component supply chain risk management.

Criteria for success and desired outcomes: Software development tool sets and processes that enable financial applications to be developed and maintained with measureable improvement (order of magnitude improvement) in their resilience (ability to operate in the face of successful attacks) and resistance (ability to prevent compromise by known and projected threats). These applications need to operate, at transaction volumes that can exceed hundreds of millions transactions a day, possibly magnified by denial of service attacks by two orders of magnitude or more. Corresponding criteria is the ability to spot counterfeit or tampered devices and software in real-time, with traceability back to the source of creation or tampering with a high order of confidence.

8. Testing Financial Applications

Current approaches to testing systems fail to catch vulnerabilities; especially if the vulnerability is new and not yet seen in the wild (e.g. zero day vulnerabilities). These vulnerabilities exist at the system, process, architecture design, update and coding level.

We need more effective and affordable security testing tools, practices and procedures in order to better manage risk and improve the security of our fielded systems and applications. The testing should include not just the application software but the hardware platforms and operating systems, people, and processes.

Testing should occur not just at one point in time but over the entire lifecycle. It should include the entire supply chain, starting where the software and hardware are first manufactured and shipped.

Testing needs to be more automated so it can simulate and test a greater number of conditions, attacks and situations.

It should test, not just how well the system runs when used in the ways it was designed to be used, but how well it works when it is used in new and unexpected ways, and with exception processing.

It should also be able to test the various interdependencies between this and other systems – what if other supporting and interdependent systems and processes break down, how will they impact the system being tested (for example, if a trading system works as designed but funding, settlement or credit processes supporting it don't work as expected)?.

Research areas include (but are not limited to):
(a) Methods for discovering and simulating new attack vectors and failure modes and for finding new vulnerabilities
(b) Automated aids to help analyze and test system process and coding logic, both static and dynamic run time performance
(c) New novel testing tools that can advance the state of the art of testing, such as instrumenting applications with the goal of recognizing attack patterns, incorporating the concepts of game theory; running more realistic test scenarios and simulations that are capable of adapting, learning and improving over time.

Criteria for success and desired outcomes: Methods of testing and assessing the security, resilience and resistance to attack of financial applications and systems that provide a measurable improvement in the ability to both identify vulnerabilities for various attack vectors to succeed, along with comprehensive analyses of areas needing improvement.

9. <u>Training</u>

We need to improve cyber education to create a more cyber savvy, security-aware workforce and customer base. It is particularly critical that we can recruit and train our security professionals. The cyber security professional trained in needed cyber defense skills is in short supply. We need help in attracting and increasing the available skilled cyber security workforce. One way is through innovative approaches to training.

Research areas include (but are not limited to):

(a) Better teaching and automated training in methods of recognizing and responding to adversary behavior. This includes investigation of technologies such as: Artificial Intelligence, MOOC (Massive Open On-line Course)[37] and Gamification[38]

(b) Ways to better identify employees with the aptitude for becoming a skilled cyber security professional

(c) New novel ways to provide on-the-job training through simulation, modeling and exercises, and context sensitive security-aware training tools built into our systems and applications.

Criteria for success and desired outcomes: A new training methodology and ways of measuring the effectiveness of this training that demonstrates a measureable improvement in the skills and readiness of our security professionals, and users, against a standardized yardstick that can result in demonstrable improvement in the effectiveness of the enterprises' security defenses. This training needs to take into account the unique systems architecture, vulnerability and regulatory compliance requirements of the financial services industry.

10. Architecture

The financial sector cannot mount an effective cyber defense in isolation. Instead, it must set reasonable expectations that the Financial Services Sector may have for Internet ecosystem technology providers who may or may not be traditional business partners for the financial services industry. These businesses include, but are not limited to: advertising services, anti-malware vendors, application stores, certificate authorities, domain name service registrars, email hosts, the Internet Corporation for Assigned Names and Numbers, Internet Service Providers, mail user agent vendors, operating system vendors, web browser vendors, web browser plug-in vendors, web server hosts, and critical infrastructure regulators. It also includes critical technology components such as cryptologic systems (it is important to support continued research in the area of cryptology and companion fields, to ensure the viability of current solutions against advances in computer technology, such as quantum computing, massively parallel processing and advanced computer algorithms, which could necessitate new, innovative approaches to protecting the confidentiality and privacy of data at rest and in motion, as well as ensuring the viability of authentication of people and digital objects.

It is easy to identify technology controls that these providers may reasonably be expected to perform in order to minimize potential damage due to malware.[39] It is more difficult to specify overall Internet security improvements that require coordination of features deployment across multiple players in this landscape that can be claimed to demonstrably improve the capability of the Financial Services Sector to deflect cyber-attacks. Such research would also involve developing game plans for how we can collectively operate in the face of degradation and loss of some of the Internet ecosystem services we may be mutually dependent upon.

[37] http://en.wikipedia.org/wiki/Massive_open_online_course

[38] http://en.wikipedia.org/wiki/Gamification

[39] See: BITS, *Malware Risks and Mitigation*, 2011, The Financial Services Roundtable: www.bitsinfo.org.

Criteria for success and desired outcomes: The minimal expectation for any successful project in this area would be formal and/or informal models of the Internet Ecosystem that can be used to test control improvements in disparate areas and show the security impact on the Financial Services Sector. Such models should allow a plug-and-play approach to modeling proposed security advances in ecosystem components in order to forecast the impact of proposed improvement deployments. Such models should realistically represent controls at each eco-system component in order to model control failure as well as improvements. Ideally these models would be useful in identifying collective accountability for control operations, and may become the basis for contractual obligations for security controls in the domain of Internet services.

Summary and Next Steps

We have provided an overview of the needs of the financial services sector for R&D targeted at meeting sector requirements for critical infrastructure protection. We hope we have succeeded in establishing a research agenda that clearly communicates these requirements to both the research funding program managers and researchers. The research areas are meant to be illustrative and not meant to rule out other research areas that could help meet our requirements. We are interested in learning about research initiatives that address these needs and to engage with the researchers and research program managers to answer any questions, provide subject matter expertise, and help transition promising research to practice in the financial services domain. These potential solutions will need to address the existing financial services operating environment, and unique regulatory, migration and cost considerations. Researchers who wish to present initiatives that support this agenda are encouraged to contact Dan@fsround.org or bob.blakely@citi.com.

Appendix A – Members of FSSCC R&D Committee

Aaron Wiessenfluh, BATS
Jennifer Bayuk, Citi
Bob Blakley, Citi
Dan DeWaal, Options Clearing Corp
Doug Johnson, ABA
Greg Gist, Citi
Jane Kung, Morgan Stanley
Jennifer Bayuk, FS-ISAC rep
Jim Devlin, Citi
John Carlson, BITS
John Oliver, State Street
Justin Peavey, Omgeo
Joel Van Dyk, DTCC
Mark Merkow, PayPal
Marlene Roberts, FDIC
Dan Schutzer, BITS
Paul Smocer, BITS
Richard Parry, JPM Chase
Bob Vitali, Morgan Stanley
Steve Earl, National Futures Association
Stephen Ward, JPM Chase
Terry Escamilla, Travelers