DTCC

Securing Today. Shaping Tomorrow.℠

CYBER RISK – A GLOBAL SYSTEMIC THREAT

A White Paper to the Industry on Systemic Risk • October 2014

TABLE OF CONTENTS

FOREWORD

In the past few years, DTCC has expanded its risk management efforts by taking a proactive approach to systemic risk identification, to either help avoid or reduce systemic repercussions in the market, where feasible.

While systemic risks are numerous and unpredictable in nature, there is growing concern about the threats, both to the financial system and to the global economy, posed by cyber attacks. In line with other industry surveys, the results of DTCC's Systemic Risk Barometer surveys indicate that cyber risk is a top industry concern for many leaders in business and government worldwide.[1]

DTCC places an extremely high organizational focus on mitigating this issue. The publication of this new systemic risk white paper underscores our commitment to addressing cyber risk. DTCC has robust internal cybersecurity policies and procedures and actively participates in industry-coordinated exercises aimed at increasing resilience against cyber attacks.

At the same time, DTCC recognizes that the systemic risk posed by cyber threats can only be mitigated by a truly coordinated approach that includes both the private and the public sector across industries and national borders. We must defend collectively or we will fail individually.

The goal of this paper is to promote dialogue on the rapidly evolving spectrum of cyber threats as a way to help determine what should be done by the various stakeholders involved to mitigate these risks. To this end, we offer a series of recommendations for consideration by the global policymaking community and industry participants.

As such, this paper is intended as a resource for DTCC's Members, policymakers and other stakeholders throughout the industry at large. We hope you share this paper with your colleagues and join the dialogue DTCC will be continuing in the coming months and years on this important issue.

Mark Clancy
DTCC Chief Information Security Officer

Michael Leibrock
DTCC Chief Systemic Risk Officer

[1] *http://dtcc.com/~/media/Files/Downloads/issues/risk/Systemic_Risk_Summary_Report.ashx*

EXECUTIVE SUMMARY

While DTCC is primarily concerned about risks that can affect the stability and integrity of the financial system it supports, it recognizes that the scope of cyber risks extends well beyond the financial world. By their nature, cyber threats cannot be addressed in isolation – they are multi-faceted risks that affect interconnected institutions large and small across industry sectors and national borders.

To effectively deal with this growing threat, it is critical, as the saying goes, to "know thy enemy." To this end, **the introductory section of this paper provides a short overview of the evolution of cyber threats** and the corresponding tools developed to address them.

Throughout this evolution, it has become clear that a robust cybersecurity regime depends on several pillars, which are described in the main sections of this paper:

- **Part One covers institutional cyber resilience** by focusing on the immediate need for institutions to develop, execute and enhance programs aimed at protecting their core business functions. This section identifies the components of high-maturity cybersecurity programs, which form the foundation for developing a more comprehensive set of partnerships and community-based actions.

- **Part Two highlights the importance of public-private partnerships** to protect against cyber threats. This section describes DTCC's role in various councils and other partnerships across the industry and also outlines DTCC's collaboration with government agencies such as the US Departments of Treasury and Homeland Security. This section also introduces Soltra, a new DTCC joint venture aimed at mitigating cyber risks across the financial industry.

- **Part Three provides a global overview of public policy initiatives** designed to safeguard critical infrastructure, protect national security and ensure data privacy. This section compares approaches taken by various jurisdictions across the globe and describes ongoing policy debates.

- **Part Four offers recommendations for addressing future cyber threats.** Drawing on best practices and lessons learned by cyber defenders, this section builds on recent trends to provide a series of forward-looking policy and industry recommendations aimed at enhancing systemic cyber resilience in the face of ever-evolving threats.

INTRODUCTION

> “[…] successful attacks on our financial system would compromise market confidence, jeopardize the integrity of data, and pose a threat to financial stability.” – Treasury Secretary Jacob Lew during a speech delivered on July 16, 2014

Since the appearance of the notorious “Morris” computer worm in the late 1980s, cyber risk has grown from a relatively isolated data center problem to a top concern among senior executives in corporate boardrooms around the world.

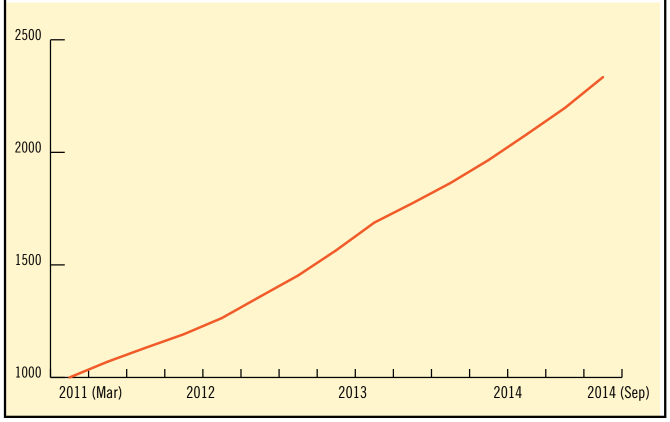
A worldwide survey by Kaspersky Lab and B2B International indicated that **93% of financial services organizations experienced various cyber threats** in the 12-month period between April 2013 and May 2014.[2] Although the financial industry was among the first to be targeted by early cybercriminals, today cyber threats extend well beyond the financial sector.

In addition to the cost of cybercrime, it is also important to acknowledge the potential systemic impact that a cyber attack could have on national and economic security. Given the critical and interconnected nature of the financial system, DTCC identified cyber risks as *“arguably the top systemic threat facing not only the global financial markets and associated infrastructures, but also world governments and military establishments”* in its 2013 Systemic Risk White Paper.

This view was confirmed by DTCC’s Systemic Risk Barometer survey in October 2014. Cyber threats were cited by 84% of respondents as one of their top 5 concerns (up from 59% in March 2014 and 45% in 2013) and 33% of respondents ranked it as the number 1 risk out of 20 choices.[3] These results are in line with a 2013 report by the International Organization of Securities Commissions, which revealed that 89% of exchanges viewed cybercrime in securities markets as a potential systemic risk.

Also noteworthy is the evolution of the **Index of Cyber Security,** as pictured to the right. This index aggregates the views of information security professionals as expressed through monthly surveys. It is a sentiment-based measure of cyber threats to the corporate, industrial and governmental information infrastructure. Based on this measure, the risk presented by cyber threats has doubled in the past 3 years.[4]

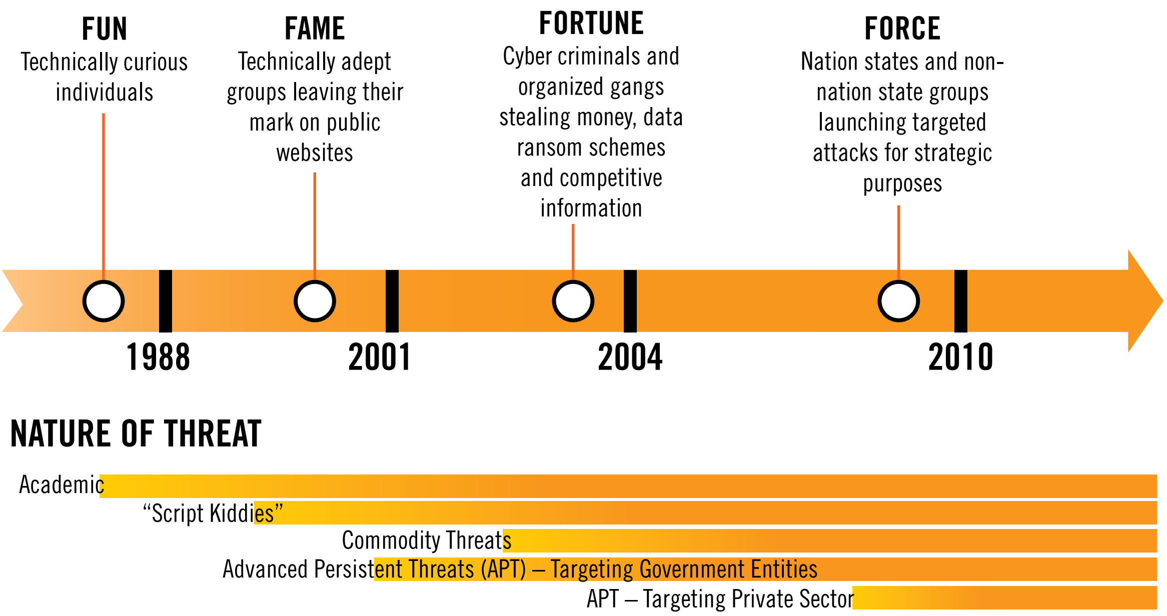
INDEX OF CYBER SECURITY



[2] http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Financial_Security_report.pdf
[3] http://www.dtcc.com/~/media/Files/Downloads/issues/risk/Systemic_Risk_Summary_Report.ashx
[4] http://www.cybersecurityindex.org/

The rise of cyber threats is a direct result of the dramatic evolution of offensive cyber weapons and techniques witnessed in the past two decades. **Cyber attacks and corresponding defenses have evolved in successive phases,** which each represent major shifts in the objectives of cyber attackers:

EVOLUTION OF CYBER ATTACKS


FUN
Technically curious individuals
FAME
Technically adept groups leaving their mark on public websites
FORTUNE
Cyber criminals and organized gangs stealing money, data ransom schemes and competitive information
FORCE
Nation states and non-nation state groups launching targeted attacks for strategic purposes
1988
2001
2004
2010
NATURE OF THREAT
Academic
"Script Kiddies"
Commodity Threats
Advanced Persistent Threats (APT) – Targeting Government Entities
APT – Targeting Private Sector

Phase 1: Fun

The first widely documented attack on networked computers involved a worm released in November 1988 called the "Morris" worm, which featured self-replicating code that exploited vulnerabilities in the email server software "Sendmail." Media reports indicated that the motivation for this attack was based largely on the author indulging in intellectual curiosity and exploring whether such an act was possible. The worm caused delays and congestion across large portions of the network known today as the Internet.

Defenders of information networks responded to this threat by sharing information with their peers about the worm, including methods for how to purge it from their systems. Ironically, this information sharing often involved the use of email, which in some cases was delayed by the propagation of the worm itself. Prior to this time it was rare for networks to be segregated using firewalls, which have now been adopted as standard practice by cyber defenders globally.

Phase 2: Fame

The second evolutionary phase of cyber threats coincided with the increased use of electronic mail and word processing tools witnessed throughout the 1990s, which was followed by an escalation of widespread attacks using computer viruses and worms. This culminated in the rise of two large-scale self-propagating worms in 2001: the first, known as "Code Red," appeared in July of 2001 and the second, known as "NIMDA," was released a week after the September 11, 2001 terrorist attacks on the United States. Both significantly damaged the availability of commercial networks by propagating rapidly through the exploitation of vulnerabilities in commonly used web server software and operating systems. The authors of these worms took credit via pseudonyms with the motivation of gaining notoriety and fame.

The primary response among defenders of networks was the realization that improved "system hygiene" – staying current on patches, configurations and software updates to their IT systems – is as critical to cybersecurity as internal and external firewalls. Indeed, maintaining system hygiene remains one of the top ongoing challenges among IT operators today. In addition, network defenders also recognized the critical importance of having visibility into what was happening on their networks in order to improve their understanding of when a worm or other intrusion might be in progress. This led to widespread adoption of intrusion and penetration testing for an institution's own web applications, better known today as Intrusion Detection Systems.

Phase 3: Fortune

The third evolutionary phase began around 2004 when the social engineering technique now known as "phishing" began to appear in larger-scale campaigns. This technique initially targeted financial institution consumers and attempted to trick individuals into disclosing passwords, identity information and payment card credentials that would allow attackers to commit fraud. This activity was, and still is, clearly motivated by financial gain.

In response, defenders realized they needed to both improve the resilience of their systems and business processes and increase their understanding of who was attacking them, what the underlying motivation really was and how the attackers were attempting to achieve their goals. This led to the adoption of technology for stronger authentication, risk-based decision systems on transactions and sharing of information about these threats, even among competitors. Critically, this collective realization helped to establish cybersecurity as a key non-competitive area within the financial services industry, which continues to enhance the industry's resilience to cyber attacks today.

THE COST OF CYBERCRIME

$400
Billion

A June 2014 report ("Net Losses – Estimating the Global Cost of Cybercrime") published by the Center for Strategic and International Studies and sponsored by McAfee estimates that cybercrime costs businesses approximately $400 billion worldwide, with an impact on approximately 200,000 jobs in the United States alone.

$3
Trillion

The World Economic Forum and McKinsey & Company examined the impact of cyber attacks and response readiness in a January 2014 report ("Risk and Responsibility in a Hyperconnected World"). The report estimates that by 2020, technological innovations worth up to $3 trillion could be left unrealized if rising cyber attacks delay their adoption.

Phase 4: Force

The fourth evolutionary phase began in 2007/2008 with the distributed denial of service (DDoS) attacks launched against Georgia and Estonia, but escalated in 2010 with the disclosure of a destructive cyber attack – known as Stuxnet – that targeted uranium refining efforts in Iran. This attack targeted specific vendors' industrial control software and used complex techniques to exploit previously unknown vulnerabilities and circumvent countermeasures, such as digitally signed software components. Around the same time, financial institutions became the target of cyber espionage attempts, which have been widely called Advanced Persistent Threats (APT).

Cyber espionage was present in the defense industry as far back as the late 1990s, but only became highly visible outside the defense sector in 2010, after Google was targeted by an attack campaign known as "Aurora." The combination of DDoS attacks, destructive cyber weapons and espionage moving beyond sole utilization by nation-states can best be described as the "Projection of Force" phase.

Phase 5: Looking Ahead – What's Next?

Symantec's 2014 *Internet Security Threat Report* named 2013 the "Year of the Mega Breach" as cybercriminals unleashed the most damaging series of cyber attacks in history.[5] Increasingly sophisticated and ever-evolving cyber attacks have led to high-profile data breaches at household names like eBay, retail giant Target, Google/Gmail, The New York Times, Neiman Marcus, Twitter, among many others – affecting more than 100 million customer accounts. In April 2013, hackers drove down the Dow Jones Industrial Average by more than 100 points within three minutes, temporarily erasing roughly $130 billion of value from US stock markets, by hijacking the Associated Press's Twitter account and issuing a false news alert that there had been an attack on the White House.

[5] *"Internet Security Threat Report 2014: Volume 19." http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf*

The techniques, tactics and procedures used to date are still in the early stages of targeting the financial system and other critical infrastructures. So far, the impact of distributed denial of service attacks against US banks and credit unions has been limited to overwhelming systems and forcing some web sites to temporarily go offline. But what if these attacks would penetrate core systems and disrupt crucial operational functions?

We can only guess what will be the next stage in this evolution. But it is worth considering the ramifications of attackers taking inspiration from non-malicious incidents within market infrastructures – such as "flash crashes," runaway trading algorithms or the issues affecting the Securities Information Processor (SIP) – and combining them with current offensive tactics. What would the effect be on global financial markets if these were not isolated events due to 'glitches' but instead were induced failures intended to occur on purpose? What will the future hold if we don't improve our resilience now?

PART ONE – INSTITUTIONAL CYBER RESILIENCE

1.1. Intelligence-Driven Defense

With the exception of the defense sector, private industry – particularly the financial services sector – has long been on the leading edge of cybersecurity efforts.

As institutions seek to address ever-evolving cyber threats, it is critical that they invest in personnel, processes and technology to understand and monitor the various threat actors who may be motivated to disrupt core business functions. No single institution faces exactly the same mix of adversaries, attack motivation or threat capabilities. In response to these variables, institutions are increasingly adopting "intelligence-driven defense" to build specific countermeasures to the threats they face.

Government cybersecurity expert Richard A. Clarke uses the acronym "CHEW" to refer to a taxonomy of cyber threats consisting of Criminals, Hacktivists, Espionage and War, with distinct motivations, capabilities and intent:

CRIMINALS

MOTIVATION:
Money
- Large number of groups
- Skills from basic to advanced
- Present in virtually every country

POTENTIAL DAMAGE:
Millions of Dollars

HACKTIVISTS

MOTIVATION:
Protest/Revenge
- Large number of groups
- Groups tend to have basic skills with a few 'standout' individuals with advanced technical and motivational skills

POTENTIAL DAMAGE:
Millions of Dollars

ESPIONAGE

MOTIVATION:
Acquiring national security secrets or economic benefit
- Small but growing number of countries with capabilities
- Larger array of 'supported' or 'tolerated' groups

POTENTIAL DAMAGE:
Hundreds of Millions of Dollars

WAR

MOTIVATION:
Politics/destroy, degrade or deny an adversary's capabilities
- Small but growing number of countries with capability
- Non-state actors may utilize 'war' like approaches

POTENTIAL DAMAGE:
Billions of Dollars

Effective intelligence-driven defense requires defenders to actively hunt for potential intrusions in their environments using all available intelligence about known techniques. It also necessitates the analysis of large quantities of data about the operating conditions of an organization's IT environment in order to identify previously unknown attack methods.

In addition to better understanding the attacker, intelligence-driven defense also recognizes that it is not possible to prevent all intrusion attempts. It requires a mindset change from "if we build walls high enough we can keep the bad guys out" to "let's assume the bad guys are already inside." Rigorous planning for an effective response is also essential, so that when attackers are discovered inside the network, the defenders can be nimble in their ability to respond and evict attackers.

1.2. Attributes of High-Maturity Cyber Defense Programs

In the present cyber threat landscape, high-maturity cyber defense programs consist of five main components:

1) Internet Threat Mitigation: One key area for financial institutions is their Internet presence. For many financial firms the Internet is an important means of conducting business as well as a representation of their brand. State-of-the-art carrier mitigation services, which detect surges in Internet activity to identify a potential attack, are a key component of protecting a firm against DDoS attacks. This service, which can be provided by an institution's Internet provider, can also steer malicious traffic away while allowing access to known users.

2) Perimeter and Internal Network Protection Enhancements: Another cybersecurity aspect features increased reliance on actively hunting for cyber threats at an organization's perimeter and within its internal environment. Building a high-maturity defense program requires both internal capabilities and outside information, which can generally be gathered from three different types of sources:

- **Community-driven sources,** such as the Financial Services Information Sharing and Analysis Center ("FS-ISAC") which enables bi-directional sharing of information, such as the technical indicators of compromise from attempted intrusions at other financial firms.
- **Government sources,** including the Department of Homeland Security's ("DHS") US Computer Emergency Response Team; the National Cybersecurity and Communications Integration Center; the FBI's Domestic Security Alliance Council Cyber Watch; and the US Secret Service Electronic Crimes Task Forces. These groups publish information from government sources and critical infrastructure service providers.
- **Commercial providers,** comprising numerous commercial intelligence services that focus on specific industries or types of threat actors.

The combination of these sources provides cyber defenders with a wider perspective as to what is occurring in the external threat landscape as well as what is possible in their institution's own environment. The information from these sources becomes "actionable" when the institution can take these indicators and feed them into systems that constantly sweep and monitor their network for indications that a system may have been compromised by known malicious software or is communicating with a hostile location. The most mature organizations also share indicators of compromise with their community sources to enrich that community's collective defense.

It is also critical that financial institutions adopt industry standards for software vulnerability enumeration and vulnerability impact scoring, known as Common Vulnerabilities & Exposures ("CVE") and Common Vulnerability Scoring System ("CVSS") respectively. The CVSS scores for all vulnerabilities are aggregated into a single number tracked by senior IT management. Should the score rise above a predetermined risk level, IT resources are shifted from day-to-day operations to activities that will bring the score down to an acceptable risk level as soon as possible.

3) Redundant IT Infrastructure – Physical vs. Cyber Event: In the post-9/11 era, financial institutions and market infrastructures have increased their resilience to catastrophic physical attacks by maintaining data centers, operational hubs and key business applications in multiple geographic regions. The development of highly redundant IT infrastructure with near real-time data replication for in-region and out-of-region data centers is critical, as it allows for almost instantaneous recovery from a catastrophic failure at a specific data center.

However, cyber attacks that corrupt the integrity of critical data can cross regions as the corrupted data may be replicated to backup locations by the infrastructure designed to add resilience for physical attacks. Although to date physical incidents such as terrorist attacks, extreme weather or blackouts have been more frequent than destructive cyber attacks, it is time that market infrastructures and their participants apply the same thinking and capabilities to extreme but plausible cyber attack scenarios.

It is essential to note that there must be "upper bounds" to extreme cyber scenarios beyond which a market infrastructure could not recover. In physical scenarios, such upper bounds are implicit – e.g., a major armed conflict that destroys the world-wide primary and back-up processing capabilities of a market infrastructure would qualify as a non-recoverable scenario, while resilience within a single geographic region could be considered a more plausible upper bound. While there are some equivalent implicit upper bounds in extreme but plausible cyber scenarios, they should be further discussed and debated by market infrastructure operators, participants and regulators as cyber threats continue to evolve.

4) Protection against Advanced Persistent Threat ("APT") Attacks: APT actors are a growing concern among critical infrastructure sectors and must be addressed head-on. These actors are generally nation-states that have highly capable intelligence, military and educational organizations that they use to achieve national-level goals such as economic security, industrial competitiveness and, in extreme cases, military advantage in conflict. This allows them to bring the full resources of a nation to bear against a target they perceive to be able to further one of these goals. In the context of cybersecurity, this means using advanced tradecraft and malware to penetrate a network to gather information or degrade it, as the needs of the nation dictate. APT actors have recently expanded their targeting from government entities to defense contractors such as Boeing and Raytheon and finally to private corporations such as Google and Exxon.

The disparity between the resources a private corporation can expend to defend and those which a nation-state can bring to attack practically ensures that the nation-state will be successful.

One of the characteristics of APT actors is that they establish a foothold in one system and then expand their access vertically with additional administrative privileges and horizontally to adjacent systems. This allows them to remain inside a network even if the initial entry point is discovered and remediated. For network defenders, the implementation of a network segmentation strategy can take advantage of this horizontal propagation and can help detect and remediate intrusions to minimize damage.

5) Market Infrastructures Leverage Private Communications Networks: Market infrastructures often utilize private networks for their high-value or high-volume communications with counterparties. These private networks provide greater availability and higher resilience against attacks such as denial of service. DTCC maintains a private data network that is separate from the Internet and that is used by many of our participants.

1.3. DTCC's Perspective

In 2012, the US Financial Stability Oversight Council unanimously designated DTCC's clearing and depository subsidiaries as Systemically Important Financial Market Utilities ("SIFMUs"). This designation subjects organizations to heightened oversight and imposes stringent risk management standards to promote safety and soundness, reduce systemic risk and support the stability of the broader financial system.

As such, DTCC places an extremely high organizational focus on mitigating the systemic risks associated with cyber threats. DTCC's cyber resilience program, which incorporates the components described above, is only one aspect of its comprehensive efforts to mitigate cyber threats to the financial industry as a whole. The other aspects, which are built around industry-coordinated partnerships and support of public policy efforts, are highlighted in subsequent sections of this paper.

PART TWO – THE IMPORTANCE OF PUBLIC-PRIVATE PARTNERSHIPS

The key to enhancing cyber resilience is building partnerships between stakeholders to collectively develop and enhance tools and resources to mitigate cyber threats. Collaborative information sharing is a key component of these partnerships, which should include industry participants, governments, universities and other private- and public-sector stakeholders.

DTCC is directly engaged in ongoing collaborative efforts with the wider financial services industry, as well as with US and European government agencies.

A further component of these efforts is the industry's already robust ability to share cyber threat information among financial institutions and with other sectors, including relevant government agencies. To augment this capability, DTCC recently joined forces with the Financial Services Information and Analysis Center ("FS-ISAC") in a joint venture known as Soltra.

2.1. Financial Services Sector Coordinating Council

The financial services sector learned long ago that cyber threats present critical common challenges and that cybersecurity is a prime area for cooperation. DTCC works collaboratively across the industry to identify potential threats and techniques to mitigate them. A key organization in this respect is the **Financial Services Sector Coordinating Council ("FSSCC").**

The FSSCC's mission is to strengthen the financial sector's resilience against cyber attacks and other threats to the nation's critical infrastructure by proactively identifying threats and promoting protection, driving preparedness and collaborating with the US government. The Council's leadership is composed of industry utilities and operators, as well as industry associations such as the Securities Industry and Financial Markets Association ("SIFMA"), the Financial Services Roundtable ("FSR") and the American Bankers Association ("ABA").

The Council has over 60 volunteer member associations and financial institutions representing clearinghouses, commercial banks, credit rating agencies, exchanges/electronic communication networks, financial advisory services, insurance companies, financial utilities, government-sponsored enterprises, investment banks, merchants, retail banks and electronic payment firms. During the past decade, the partnership has continued to grow, both in terms of the size and commitment of its membership and in the breadth of issues it addresses. Members commit their time and resources to FSSCC with a sense of responsibility to their individual firms and for the benefit of financial consumers and the nation.

The FSSCC is considered the policy arm of the financial sector in terms of its engagement with the public sector and other critical sectors of the economy. As such, it dedicated much of 2013 to responding to Executive Order 13636 *Improving Critical Infrastructure Cybersecurity,* particularly regarding the development of a Preliminary Cybersecurity Framework under the leadership of the National Institute of Standards and Technology ("NIST").

2.2. Financial Services Information Sharing and Analysis Center

Also critical to DTCC and the industry's cybersecurity capabilities is the **Financial Services Information Sharing and Analysis Center ("FS-ISAC"),** which serves as the operational arm of the FSSCC and as the primary communications channel for the financial services sector. FS-ISAC also recently took over the role of coordinating crisis response for the financial services sector (formerly a responsibility of FSSCC), which has injected additional operational capabilities into the response process.

The FS-ISAC was established by the financial services sector in response to Presidential Directive 63 issued in 1998. This Directive sought to address critical infrastructure vulnerabilities by, among other things, designating lead agencies to improve public-private coordination in each sector. In 2003, that Directive was superseded by Homeland Security Presidential Directive 7 and in 2014 by Presidential Policy Directive 21, which directed both public and private sectors to share information about physical and cyber threats and vulnerabilities to help protect the US critical infrastructure.

The FS-ISAC is focused on implementing these Directives and protecting the financial services sector. It acts as a trusted third party that provides anonymity to allow members to share information in a non-attributable and trusted manner. The FS-ISAC provides a formal structure for valuable and actionable information to be shared among members, the sector and its industry and government partners, which ultimately benefits the nation. FS-ISAC's information sharing services and activities include:

- Delivery of timely, relevant and actionable cyber and physical email alerts from various sources and an anonymous online submission capability to facilitate member sharing of threat, vulnerability and incident information in a non-attributable and trusted manner through the FS-ISAC Security Operations Center (SOC).
- Support for information exchanges with various special interest groups including the FSSCC; the FS-ISAC Threat Intelligence Committee; the Payment Processors Information Sharing Council (PPISC); the Clearing House and Exchange Forum (CHEF); the Business Resilience Committee (BRC); and the Payments Risk Council (PRC).
- Development of risk mitigation best practices, threat analysis, toolkits and the preparation of cybersecurity briefings and white papers.
- Development and testing of crisis management procedures for the sector in collaboration with the FSSCC and other industry bodies.

GLOBAL PARTNERSHIPS IN THE FINANCIAL SECTOR

The World Federation of Exchanges established a cybersecurity working group to bring the world's stock exchanges together to address the specific threats market infrastructures face. The group – called GLEX for GLobal EXchange security – is an information sharing and advocacy hub for large and small exchanges across the globe.

2.3. Executive Branch Agency Collaboration

2.3.1. US Department of Treasury

In an effort to balance the need for security and the normal operations of sectors in the post-9/11 landscape, Sector Specific Agencies ("SSAs") were designated for critical infrastructure sectors. In the case of the financial services sector, the US Department of Treasury functions as the SSA, serving as the "go to" agency for the sector's interaction with the US government.

Treasury Secretary Jacob Lew described the role of the Treasury Financial Sector Cyber Intelligence Group as a key component of this partnership in a speech he delivered in July 2014:[6]

> *"To increase information sharing across the financial services industry, Treasury has created an information sharing and analysis unit, known as the Financial Sector Cyber Intelligence Group. This team is delivering timely and actionable information that financial institutions can use to protect themselves. This unit consists of cyber experts and security analysts who scour law enforcement and intelligence reports constantly to find relevant activity, analyze and connect the dots between events, and issue information bulletins for security professionals in the financial sector."*

[6] *http://www.treasury.gov/press-center/press-releases/Pages/jl2570.aspx*

Additionally, through the FSSCC and the FS-ISAC, DTCC also interacts with the Financial and Banking Information Infrastructure Committee ("FBIIC"), which is led by the US Department of the Treasury and chartered under the President's Working Group on Financial Markets. FBIIC is charged with improving coordination and communication among financial regulators, enhancing the resilience of the financial sector and promoting the public-private partnership. The public sector's commitment to the public-private sector partnership outside of the already mature regulatory regime is essential to FSSCC's success.

2.3.2. US Department of Homeland Security

Part of DTCC's broader relationship with the Executive Branch is its collaboration with the US Department of Homeland Security ("DHS"). As part of this collaboration, DTCC works with DHS on new technology to thwart cyber attacks and also participates in the critical infrastructure protection program. As a critical infrastructure operator, DTCC actively supports and engages with the National Cybersecurity & Communications Integration Center ("NCCIC") at DHS. The NCCIC's mission is to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the nation's critical information technology and communications networks.

2.4. Soltra

As mentioned previously, DTCC joined forces with the FS-ISAC in early 2014 to launch a Cyber Threat Intelligence initiative known as *Soltra*. The purpose of this initiative is to develop and distribute a software application and create a network for the automated sharing of security intelligence to protect critical infrastructures.

The cyber intelligence sharing industry is a relatively new market that has emerged over the past two to three years. This market focuses on creating communities of trust that share threat information. In most cases, threat information is defined as lists of malicious file hashes, URLs, domains or IP addresses. To increase trust, participants in this space typically allow for threat analysts to collaborate and communicate across individual companies and sectors. This trust model began with face-to-face information sharing between persons, but evolved into institution-to-institution information sharing via ad-hoc sharing portals.

At present, the trust model needs to evolve to a point where standard message formats are used for infrastructure-to-infrastructure information sharing in real time. The need for real-time threat sharing in a trusted community is faced by all critical infrastructures globally and the SoltraEdge solution is designed to serve multiple industries and geographic regions of the world.

Soltra is centered on a fully automated computer-to-computer solution that encourages the use of straight-through processing. Information pertaining to cyber threats would be electronically entered and transferred between parties without manually re-entering data, thus creating efficiencies in an environment where it is vital to convey important information quickly.

SoltraEdge will allow clients to read and write information using the STIX specification (Structured Threat Information eXpression) and transmit and receive data using the TAXII specification (Trusted Automated eXchange of Indication Information). SoltraEdge will support peer-to-peer communications to other SoltraEdge users via TAXII, essentially creating a community forum for cyber threat information.

The adoption of STIX/TAXII will allow Soltra to build a specifications-based ecosystem. Other approaches mostly focus on cloud implementations that move cyber intelligence sharing software from internal controls, thus increasing the complexity to integrate. The cloud focus requires intelligence to be hosted in the cloud, which also raises privacy concerns for clients.

The soft launch for Soltra was implemented in the summer of 2014 with roughly 45 clients in a pilot. The full launch is scheduled to take place in Q4 2014. Additional information can be found on *http://www.soltraedge.com*

PART THREE – PUBLIC POLICY INITIATIVES

> “[…] there can be little doubt that cyber risk also must be considered as part of a board’s overall risk oversight.”
>
> – SEC Commissioner Luis A. Aguilar during a June 10, 2014 speech at the New York Stock Exchange

Policymakers around the world are increasingly undertaking efforts to address cyber risks. These efforts include the definition of critical infrastructure and the development of cybersecurity strategies that incorporate both the private and public sectors.

While specific approaches and objectives vary by jurisdiction, efforts to date have focused on four main areas of concern:

- enhanced protection of national critical infrastructure;
- improved information sharing between the public and private sectors and corresponding liability protections;
- data breach notifications; and
- data privacy issues.

The design and direction of cybersecurity policymaking initiatives have largely hinged on striking the right balance between enhancing critical infrastructure protection and ensuring individual data privacy.

This section focuses on policymaking initiatives in the United States, Europe, Asia and South and Central America.

3.1. US Cybersecurity Initiatives

The executive and legislative branches of the US government have made efforts to improve national resilience to cyber attacks. These include ongoing initiatives to protect the financial services sector and corresponding market infrastructure providers, as part of 16 critical infrastructure sectors identified by the US Department of Homeland Security. Additional initiatives have been undertaken by financial market regulators as well.

3.1.1. Executive Initiatives

President Obama declared cybersecurity a top priority during his 2008 electoral campaign and subsequently launched several cybersecurity initiatives, including the National Cyberspace Policy Review in 2009 and the International Strategy for Cyberspace in 2011.

In February 2013, the Obama administration issued **Executive Order 13636,** *Improving Critical Infrastructure Cybersecurity.* In addition to expanding an existing program for information sharing and collaboration between the government and the private sector, this Executive Order:

- established a process for identifying critical infrastructure where a cyber incident could *"reasonably result in catastrophic national effects on public health or safety, economic security or national security"*; and
- directed the National Institute of Standards and Technology ("NIST") to take the lead in developing a voluntary framework for reducing cyber risks to critical infrastructure.

The NIST Framework consists of standards, guidelines and practices to help owners and operators of critical infrastructure manage cyber risks. After a year of extensive collaboration between government and the private sector, the first version of the Framework was finalized in February 2014 and subsequently updated in August 2014. In addition to the information presented in the update, NIST released a formal Request for Information asking for further feedback (to be provided by October 10, 2014) on awareness, initial experiences with the Framework and related activities to support the use of the Framework. This indicates a continued interest by NIST to maintain a collaborative relationship with the private sector and to continue to fine-tune the Framework itself.

At the same time, the Obama Administration released **Presidential Policy Directive (PPD-21) Critical Infrastructure Security and Resilience,** which focuses on ways to evaluate and build on existing critical infrastructure public-private partnerships and identify baseline data that will enable the government to more efficiently exchange information and intelligence. It also required the update of the National Infrastructure Protection Plan to focus on security and resilience of critical infrastructure.

3.1.2. Legislative Initiatives

Several legislative initiatives to protect American critical infrastructures have been introduced in the last three Congressional sessions. These include the National Cybersecurity and Critical Infrastructure Protection ("NCCIP") Act of 2013 (H.R. 3696); the Cyber Intelligence Sharing and Protection Act ("CISPA") of 2013 (H.R. 624); the Cybersecurity Information Sharing Act ("CISA") (S. 2588); and the Cyber Information Sharing Tax Credit Act (S. 2717).

Various components of these bills include:

- Codifying into the law the role of the US Department of Homeland Security in the oversight and coordination of public-private cybersecurity efforts;
- Codifying existing federal civilian cybersecurity mechanisms as well as the NIST Framework;
- Improving information sharing between the public and private sectors and among private sector entities; and
- Bolstering liability protection for entities involved in voluntary information sharing programs.

DEFINING CRITICAL INFRASTRUCTURE

In order to adequately protect against the systemic risk of cyber threats, it is essential to appropriately define and identify critical infrastructure.

To maintain consistency between the various Executive Branch agencies charged with protecting critical infrastructure in the United States, Executive Order 13636 Improving Critical Infrastructure Cybersecurity specifically identifies the types of critical infrastructure considered "at risk."

Other major jurisdictions, including the European Union, do not currently have a clear or unified definition of critical infrastructure for the financial services sector.

The European Central Bank, the Bank for International Settlements ("BIS") and the International Organization of Securities Commissions ("IOSCO") do not formally define critical infrastructure in their respective guidance to financial institutions and regulators. Rather, the guidance issued to date focuses on the need for organizations to put programs in place to determine what people, facilities and systems are necessary for the smooth functioning of financial institutions. For example, the Monetary Authority of Singapore (MAS) has actually defined a critical system as "a system supporting essential business functions of the financial institution such that any failure will cause severe disruption to the financial institution's operations."

To date, no comprehensive cybersecurity legislation has been passed by Congress and signed into law by the President. In the age of Big Data and ongoing cyber attacks, the challenge remains to balance the needs of both the public and private sectors to address ongoing security challenges while continuing to protect individuals' privacy.

3.1.3. Regulatory Initiatives

Financial market regulators are also pursuing a number of cybersecurity initiatives:

- **In March 2013, the Securities and Exchange Commission ("SEC") held the first-ever all day roundtable meeting on cybersecurity.** This meeting focused on the cybersecurity landscape and issues such as cyber incident disclosures faced by exchanges, other key market systems, broker-dealers, investment advisers, transfer agents and public companies.
- **Also, in March 2014, the SEC proposed new rules to require certain key market participants to have comprehensive policies and procedures in place surrounding their technological systems.** The Regulation Systems Compliance and Integrity ("Reg SCI") would replace the current voluntary compliance program with enforceable rules designed to better insulate the markets from vulnerabilities posed by systems technology and information security issues. A final vote on the proposed Regulation is expected later this year.
- **In April 2014, the SEC announced its intention to begin examining the cybersecurity preparedness of market participants, particularly the IT systems at broker-dealers and investment advisers.** The SEC's Office of Compliance Inspections and Examinations issued a risk alert notifying firms it will conduct IT security examinations of more than 50 registered broker-dealers and registered investment advisers. The SEC has developed a cybersecurity document that supplies compliance professionals with questions they can use to assess their firms' state of readiness. Some of the questions track information outlined in the NIST Framework for Improving Critical Infrastructure Cybersecurity. [7]
- **Like the SEC, Financial Industry Regulatory Authority ("FINRA") also planned "sweep examinations," after announcing that cybersecurity was one of its 2014 examination priorities.** FINRA announced targeted examinations assessing broker-dealers' approaches to managing cyber threats and many of the same issues as the SEC's examinations.
- **In June 2014, the Federal Financial Institutions Examination Council ("FFIEC") created the Cybersecurity and Critical Infrastructure Working Group and announced its start of cybersecurity assessments aimed to help smaller banking institutions address potential security gaps.** The assessments will examine more than 500 community banking institutions with a focus on risk management and oversight; threat intelligence and collaboration; cybersecurity controls; service providers and vendor risk management; and cyber incident management and resilience. The FFIEC also issued a notice requiring banks and financial institutions to monitor for DDoS attacks against their networks and have a plan in place to try and mitigate the associated risks. More specifically, each institution is expected to monitor incoming traffic to its public website, activate incident response plans if it suspects that a DDoS attack is occurring and ensure sufficient staffing for the duration of the attack, including the use of pre-contracted third-party services, if appropriate.

3.2. European Union Cybersecurity Initiatives

This section focuses solely on public policy initiatives at the level of the European Union ("EU"), as opposed to efforts within individual member countries.

[7] *http://www.sec.gov/ocie/announcement/Cybersecurity+Risk+Alert++%2526+Appendix+-+4.15.14.pdf*

3.2.1. European Program for Critical Infrastructure Protection

The European Program for Critical Infrastructure Protection ("EPCIP") sets the overall framework for activities aimed at improving the protection of critical infrastructures in Europe and in all relevant economic sectors. A key pillar of this program is the 2008 Directive on European Critical Infrastructures ("ECI"), which established a procedure for identifying and designating ECI and a common approach for assessing the need to improve their protection. The Directive is currently focused on energy and transportation firms, but a new approach has emerged that foresees the identification and selection of possible pan-European infrastructures as part of a revised and more practical framework for prevention, preparedness and incident response.

3.2.2. Directive on Attacks against Information Systems

In 2013, the legislative Framework Decision on Attacks against Information Systems came into force introducing new rules and penalties, varying between two and five years of imprisonment. The Directive provides that penalties should be more severe if an attack against an information system is committed by a criminal organization or if it causes significant damage or affects key infrastructure.[8] Furthermore, EU States will have to set up a system to respond to urgent information requests with a delay of no more than eight hours. The 28 Member States have until September 4, 2015 to implement the provisions into national law.

3.2.3. The Network and Information Security Directive and the Cybersecurity Strategy of the European Union

In February 2013, the European Commission, together with the High Representative of the Union for Foreign Affairs and Security Policy, published a document describing its cybersecurity strategy *(Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace)*. The aim of this strategy is to enhance cyber resilience of information systems, reduce cybercrime and strengthen EU international cybersecurity policy and cyber defense.

Alongside its cybersecurity strategy, the European Commission also proposed a **Network and Information Security ("NIS") Directive** to ensure that critical infrastructure operators (including financial market infrastructures such as stock exchanges and Central Counterparties) meet appropriate IT security standards, share cyber threat information and notify authorities of any significant incident. The proposed Directive would also require EU countries to exchange information on such incidents and would provide implementation and enforcement responsibilities to sector-specific authorities. In particular, the draft proposal could require industry participants to undergo a security audit by a qualified independent body or national authority. The European Parliament adopted its report on the NIS Directive in March 2014 and the final text should be agreed in 2015. The implementation deadline is expected in early 2017.

As part of its cybersecurity strategy, and in order to help implement the measures set out in the NIS Directive, the European Commission has created the **NIS Platform**, a public-private partnership among more than 200 members in 18 Member States which met for the first time in June 2013. The NIS Platform, which includes representatives from research, academia and various industry sectors, is divided in three working groups to issue guidance on risk management, information sharing and incident notification. It will develop a series of non-binding Recommendations on Good Cybersecurity Practices, which will serve as a reference document for organizations seeking to improve their cyber resilience. The document is set to be released in the second half of 2015.

EUROPEAN CYBERSECURITY STATISTICS

26%

Eurostat figures show that, by January 2012, only 26% of enterprises in the EU had a formally defined information and communications technology security policy.

38%

The 2012 Eurobarometer poll on cybersecurity found that 38% of Internet users in the EU have changed their behavior because of security concerns, with 18% less likely to buy goods online and 15% less likely to use online banking.

3.2.4. Data Protection Framework/Safe Harbor

The EU is also working on a new personal data protection bill, in order to update

[8] *Firms should consult with their relevant national supervisor on the respective definition of "significant damage or affects key infrastructure."*

the current data protection framework (which stems from a 1995 agreement) and adapt it to the digital era. The European Commission released a draft package in 2012, including two legislative proposals for a Data Protection Regulation and a Directive on Police and Criminal Justice Data Protection.

The decision-making process has been delayed several times and is expected to come to a close in 2015, with implementation envisaged for 2017. Although the draft law does not represent a major shift in EU data protection policy, it includes additional enforcement and accountability requirements. Its scope has also been extended to cover the processing of all EU subjects' personal data.

The draft also introduces new requirements, such as obligatory Privacy Impact Assessments ("PIAs"), the appointment of a Data Protection Officer and mandatory data breach notifications. It also outlines what mechanisms can be used to transfer data out of the EU, especially if the third country's data protection rules are considered non-adequate.[9] Finally, the new framework introduces a harmonization element, which is a big step forward, as it facilitates cross-border business within the EU.

3.3. Asian Cybersecurity Initiatives

Large-scale cyber breaches in Asia have prompted national legislators to pursue their own policymaking initiatives. We will highlight initiatives in Japan, Australia, Singapore and India.

3.3.1. Japan

Japanese government cybersecurity initiatives are led by the Cabinet's National Information Security Center ("NISC"), which was founded in 2005. The NISC works closely with other government departments to design and implement cybersecurity policy, including incident and emergency response measures and common cyber standards and recommendations to improve cyber resilience. Japan instituted a national Cybersecurity Policy in 2013 and has been a key player in cooperative cross-border efforts to improve government and private IT security and information sharing.

Led by NISC, Japan developed a collaborative mechanism for sharing security information with members of the Association of Southeast Asian Nations ("ASEAN"), including Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. This initiative is similar to the US FS-ISAC, but restricted to ASEAN members.

3.3.2. Australia

In Australia, a key initiative involves the development of the Australian Cyber Security Centre ("ACSC"), which *"will bring together existing cybersecurity capabilities across Defense, the Attorney-General's Department, Australian Security Intelligence Organization, Australian Federal Police and Australian Crime Commission in a single location."* [10] Slated for development by late 2014, the ACSC will play a key role in coordinating cybersecurity operations and capabilities, as well as guiding national responses to cyber attacks.

Also noteworthy is the list of Strategies to Mitigate Targeted Cyber Intrusions that is published by the Australian Signals Directorate ("ASD"). The Directorate ranks these strategies in order of overall effectiveness based on its analysis of reported security incidents and vulnerabilities detected in testing the security of Australian government's networks. The ASD finds that at least 85% of targeted cyber intrusions may be prevented by following the Top 4 mitigation strategies (see Industry Recommendations in the final section of this paper). [11]

3.3.3. Singapore

Faced with its own wave of cyber attacks against government targets, Singapore has also ramped up its efforts to improve its resilience to cyber threats. In August 2014, Singapore announced its intention to upgrade its cyber capabilities through the National Cyber Security Masterplan 2018, developed by the Infocomm Development Authority of Singapore ("IDA") under the guidance of the National Infocomm Security Committee ("NISC").

[9] *According to the Safe Harbor agreement, companies operating in the EU are not allowed to send personal data to countries outside the EU without a guaranteed adequate level of protection. Such protection can either be at a state level (i.e., if national laws are considered to offer equal protection) or at an organizational level (where a multinational organization produces and documents its internal controls on personal data). The Safe Harbor Privacy Principles allow US companies to register their certification if they meet the EU requirements.*

[10] *http://asd.gov.au/infosec/acsc.htm*

[11] *http://asd.gov.au/infosec/top35mitigationstrategies.htm*

The Plan replaces the previous two policies (which ran from 2005 to 2012) and incorporates the public and private sectors into a collaborative strategy designed to protect national critical infrastructures, businesses and the general public. It also emphasizes the development of an expert IT security workforce to support future cybersecurity programs in both the public and private sectors. The IDA also recently announced an upgrade to the country's Cyber-Watch Centre by January 2015 to strengthen the government's cyber intrusion detection capabilities.

3.3.4. India

India released its National Cyber Security Policy in May 2013, which has formed the core of its efforts to unify its cybersecurity initiatives into a comprehensive program. According to the Indian Ministry of Communications and Information Technology, the key aim of the Policy is "to protect information and information infrastructure in cyber space, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation."[12] The new policy serves as an umbrella framework for entities in the private and public sectors – both large and small – as they seek to improve their cyber resilience. Consistent with other national cybersecurity frameworks, it also recognizes that cybersecurity efforts are not a "one-size-fits all" solution and acknowledges that the policy should enable various sectors to design and implement effective cyber measures that suit their specific needs.

3.4. Central and South American Cybersecurity Initiatives

Led by the Organization of American States ("OAS"), cybersecurity policymaking initiatives have recently gained momentum throughout South and Central America as well.

As part of these efforts, OAS hosted a series of events in Mexico City in July 2014, beginning with a workshop on cybersecurity and critical infrastructure protection that was designed to help policymakers develop legislative and regulatory initiatives to better protect their respective critical infrastructures. Additionally, the Inter-American Committee against Terrorism of the OAS recently carried out a cyber crisis management exercise in Montevideo, Uruguay, and hosted a workshop in Dominica to assist in the development of the country's national cybersecurity strategy.

The OAS also recently signed a Memorandum of Understanding with the Open Web Application Security Project (OWASP), a global non-profit organization focused on informing and educating users on the security risks and solutions associated with computer programming.

The Secretariat of the Inter-American Committee against Terrorism employs an integrated approach to building cyber security capacity in OAS Member States, recognizing that the responsibility for securing cyberspace lies with a wide range of national and regional entities from the public and private sectors working on both policy and technical issues.

To this end, the Secretariat seeks to:

- establish national "alert, watch, and warning" groups, also known as Computer Security Incident Response Teams ("CSIRTs"), in each country;
- create a hemispheric watch and warning network made up of these CSIRTs that provides guidance and support to cyber security technicians from around the Americas;
- cultivate and support the development of National Cyber Security Strategies; and
- promote a culture and awareness of cyber security that provides for strengthening of Cyber Security in the Americas.

[12] *http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf*

PART FOUR – ADDRESSING FUTURE CYBER THREATS

Given the ever-changing nature of cyber threats, coordination among and between policymakers and industry participants is key to mitigating cyber risks. As such, this section provides a series of suggestions for consideration by the global policymaking community, as well as a number of industry recommendations and additional resources.

4.1. Policy Recommendations

DTCC supports the ongoing efforts of policymakers around the world to move forward an aggressive agenda to combat cyber threats. Additionally, DTCC recommends:

- **Further coordinated action at all levels of government** around the world to address cyber threats and harmonize public policy. DTCC continues to engage with policymakers in the US and abroad to shape a regime that serves the dual purposes of safety and cyber resilience as well as unfettered information sharing.

- **The development of national definitions of "critical infrastructure"** in jurisdictions that have not already done so to ensure that cybersecurity programs adequately protect against cyber threats and the systemic risks they can create.

- **A harmonized and non-duplicative notification regime** that puts information sharing and cooperation among regulatory authorities and industry participants at its core.

- **Clarity in the purpose and intention of any such notification regime,** so that the content of the notice supports the objective. For example, if the purpose is consumer or investor protection, the content required to support those objectives is quite different than if the purpose is to help defenders of critical infrastructures respond to attacks. Policies that attempt to commingle all of these purposes in one notice are likely to fail.

- **An effective and collaborative information sharing regime** that enhances the financial sector's ability to prepare for and respond to cyber and physical threats, vulnerabilities and incidents.

- **The creation of global industry working groups** to work with relevant national regulators on the development of cybersecurity regulations that address the real-time and evolving nature of cyber threats. Cyber attackers currently operate on an innovation cycle that is typically measured in terms of months, which far outstrips the pace of policymaking decisions.

- **Additional efforts by policymakers to identify appropriate boundaries of responsibility** for large-scale cyber attacks against the financial services sector and other private sectors. In the age of increasing APT attacks from nation-state actors with much greater resources than their targets, private sector institutions cannot be expected to independently respond to or recover from all levels of cyber attack.

4.2. Industry Recommendations

- **Define what constitutes critical infrastructure within your organization.** In the United States, the definition included in Executive Order 13636 *Improving Critical Infrastructure Cybersecurity* provides a secure starting point. Non-US based organizations should consult with their main regulatory authority.

- **Review available cybersecurity frameworks** to determine the best fit for your organization. The NIST framework is specific to critical infrastructures and serves as an appropriate starting point. The SANS Institute's Critical Security Controls and the US National Security Agency's Top 10 Information Assurance Mitigation Strategies also offer critical guidance.[13]

- **Shift the focus of cybersecurity programs from "check the box" security to actively hunting for threats.** A cybersecurity program designed to only meet existing requirements or exclusively address known threats offers inadequate protection in today's cyber landscape. Current cyber threats evolve and move quickly and, as such, legacy methods of defending an infrastructure are likely to fail.

- **Master the mundane and maintain exceedingly high network hygiene.** The Australian Signals Directorate finds that at least 85% of targeted cyber intrusions may be prevented by following these Top 4 mitigation strategies:
  - use application whitelisting to help prevent malicious software and unapproved programs from running;
  - patch applications such as Java, PDF viewers, Flash, web browsers and Microsoft Office;
  - patch operating system vulnerabilities; and
  - restrict administrative privileges to operating systems and applications based on user duties.[14]

- **Devise a single metric that is easily understood by senior management** to encourage your IT organization to practice appropriate network hygiene. The accumulated CVSS score of vulnerabilities is an excellent metric that can be used to drive software vulnerability- patching operations.

- **Build a strong technology foundation for existing and new businesses** by leveraging configuration guidance from the Center for Internet Security (CIS). It is more cost-efficient to correctly build the foundational infrastructure once than to add security later or rebuild the infrastructure late in the product launch process.

- **Understand that prevention eventually fails** and have people, processes and technology in place to rebuild critical infrastructure. In particular, if an advanced threat actor targets your organization, it is highly likely it will succeed in penetrating your systems. Plan ahead to identify ways to deal with a major blow to your networks and systems.

Additional resources for institutions looking to enhance their cyber resilience include:

- **The NIST Framework for Improving Critical Infrastructure Cybersecurity.** This is a highly recommended guide for firms seeking to develop and enhance their cybersecurity program. As noted previously, the framework is the result of collaboration between industry and government, making it flexible and implementable by private sector organizations of all sizes.

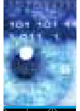
- **The NIST National Vulnerability Database and the Security Content Automation Protocol suite of tools and standards** are also excellent resources for securing technology platforms. These tools and standards allow an organization to quickly assess the environment for vulnerabilities and score them in a consistent manner to support risk-based decision-making.

[13] *The NSA's Information Assurance Directorate https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_Top10IAMitigationStrategies_Web.pdf The SANS Institute's Critical Security Controls http://www.sans.org/critical-security-controls/*

[14] *http://www.asd.gov.au/publications/csocprotect/Top_4_Mitigations.pdf?&verNov12*

- **The Center for Internet Security ("CIS")** publishes valuable Security Benchmarks for a variety of technology platforms, which have been created through private sector collaboration and consensus. The benchmarks provide best practices and technical guidance for securely configuring the various technologies while minimizing operational impact. Joining CIS provides access to machine-readable versions of the benchmarks as well as tools to automate compliance-checking. Several leading technology vendors also integrate the benchmarks into their products.

- **The Open Web Application Security Project Top Ten** is a great resource for web application security. As more and more business functions move to web-based services, securing the applications that drive these services becomes more critical. The Top Ten is a consensus document that covers what cybercriminals are attacking and that is updated every year to reflect the most recent changes. This is particularly valuable as it allows an organization to focus limited protection resources on the most likely attack points in a web application.



CONCLUSION

This paper offers some examples of actions taken by DTCC and the broader industry toward addressing a number of cyber threats. It is necessary to stress that cyber threats are dynamic by their very nature. As such, only through close engagement and action among all key participants – within the financial industry and outside of it – are we likely to achieve our collective goal of mitigating the cyber threats we face.

While substantial progress has been made in terms of public policy actions to effectively counter the ever-evolving cyber threat, further action is needed at both the national and international levels of government legislation and regulation.

We actively encourage our Members and other industry stakeholders to contribute their thoughts on the proposed mitigants and recommendations as part of the ongoing dialogue we are promoting.

Input can be provided to:

Mark Clancy, DTCC Chief Information Security Officer
mclancy@dtcc.com or +1-813-470-2400.

OR

Michael Leibrock, DTCC Chief Systemic Risk Officer
mleibrock@dtcc.com or +1-212-855-3243.

APPENDIX: GLOSSARY OF KEY TERMS

Advanced Persistent Threat (APT): A set of stealthy and continuous computer hacking processes often orchestrated by targeting a specific entity. APTs usually target organizations and or nations for business or political motives and are characterized by their escalation of technical means or constant attempts to penetrate a target until they achieve their objectives.

American Bankers Association (ABA): Part of FSSCC's leadership, a Washington, D.C.-based trade association for the US banking industry.

Australian Cyber Security Centre (ACSC): A government initiative to bring together existing cyber security capabilities across Defence, the Attorney-General's Department, Australian Security Intelligence Organisation, Australian Federal Police and Australian Crime Commission in a single location. It will create a hub for collaboration and information-sharing with the private sector, state and territory governments and international partners to combat the full breadth of cyber threats.

Australian Signals Directorate (ASD): An intelligence agency in the Australian Government Department of Defence. ASD provides information security advice and services mainly to Australian federal and state government agencies. ASD also works closely with industry to develop and deploy secure cryptographic products.

Center for Internet Security (CIS): Strives to improve global internet security by creating and fostering a trustable and secure environment to bridge the public and private sectors. CIS produces consensus-based, best practice secure configuration benchmarks and security automation content, and serves as a cyber security resource for state, local, territorial and trial governments.

Center for Strategic and International Studies: Conducts research and analysis and develops policy initiatives that look to the future and anticipate change. Has published papers and reports on cyber issues.

CHEW: Term coined by government cybersecurity expert Richard A. Clarke, the acronym refers to a taxonomy of cyber threats consisting of Criminals, Hacktivists, Espionage and War.

Common Vulnerabilities & Exposures (CVE): Standard for software vulnerability enumeration.

Common Vulnerability Scoring System (CVSS): Standard for vulnerability impact scoring.

Directive on European Critical Infrastructures (ECI): Established a procedure for identifying and designating European Critical Infrastructures and a common approach for assessing the need to improve their protection.

Distributed Denial of Service (DDoS): A distributed denial-of-service attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service on the system to legitimate users.

Domestic Security Alliance Council Cyber Watch: The Domestic Security Alliance Council (DSAC) is a strategic partnership between the US Government and US Private Industry. Cyber Watch (CyWatch) is the FBI's 24-hour command center for cyber intrusion prevention and response operations. CyWatch receives threat and incident reporting, assesses it for action, and engages with the appropriate components within Cyber Division, the field, and other intelligence and law enforcement agencies for action.

European Program for Critical Infrastructure Protection (EPCIP): Sets the overall framework for activities aimed at improving the protection of critical infrastructures in Europe and in all relevant economic sectors.

Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity: Expands existing program for information sharing and collaboration between the government and the private sector. It established a process for identifying critical infrastructure where a cybersecurity incident could "reasonably result in catastrophic national effects on public health or safety, economic security or national security" and directed the US National Institute of Standards and Technology ("NIST") to take the lead in developing a voluntary framework for reducing cyber risks to critical infrastructure.

Federal Financial Institutions Examination Council (FFIEC): A formal interagency body of the US government made up of five banking regulators, including the Federal Reserve Board of Governors (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB). It is empowered to prescribe uniform principles, standards, and report forms in order to promote uniformity in the supervision of financial institutions.

Financial and Banking Information Infrastructure Committee (FBIIC): Led by the US Department of the Treasury and chartered under the President's Working Group on Financial Markets. FBIIC is charged with improving coordination and communication among financial regulators, enhancing the resilience of the financial sector and promoting the public-private partnership.

Financial Industry Regulatory Authority (FINRA): A private corporation that acts as a self-regulatory organization that regulates member brokerage firms and exchange markets. FINRA announced targeted examinations assessing broker-dealers' approaches to managing cyber threats and planned "sweep examinations," after declaring cybersecurity as one of its 2014 examination priorities.

Financial Market Utilities (FMUs): Entities of the financial system infrastructure that aid in the role of clearing and settling transactions between financial institutions.

Financial Services Information Sharing and Analysis Center (FS-ISAC): Serves as the operational arm of the FSSCC and is the primary communications channel for the US financial sector. The FS-ISAC was established by the sector in response to Presidential Directive 63, issued in 1998.

Financial Services Roundtable (FSR): Part of FSSCC's leadership, an advocacy organization for the US financial services industry.

Financial Services Sector Coordinating Council (FSSCC): Established in 2002, FSSCC is the sector coordinator for Financial Services for the protection of critical infrastructure, focused on operational risk. FSSCC's mission is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure. The FSSCC works with the US Department of Treasury as its designated Sector Specific Agency (SSA).

Financial Stability Oversight Council (FSOC): As established under the Dodd-Frank Wall Street Reform and Consumer Protection Act, the Council provides comprehensive monitoring of the stability of the US financial system. The Financial Stability Oversight Council designates SIFMUs.

Framework Decision on Attacks against Information Systems: European Union effort to improve cooperation among judicial and other competent authorities in the area of attacks against information systems.

GLobal EXchange security (GLEX): Information sharing and advocacy hub for large and small exchanges across the globe established by the World Federation of Exchanges.

Hactivists: Threat actors. Typically nation states or hackers who are paid for the impact and damage they cause.

Index of Cyber Security: A sentiment-based measure of the risk to the corporate, industrial, and governmental information infrastructure from a spectrum of cybersecurity threats. The Index of cyber Security is a measure of perceived risk. A high index value indicates a perception of increasing risk, while a lower index value indicates the opposite.

Infocomm Development Authority of Singapore (IDA): Statutory board of the Singapore Government, formed on December 1, 1999, when the government merged the National Computer Board (NCB) and Telecommunication Authority of Singapore (TAS), as a result of a growing convergence of information technology and telephony.

National Cybersecurity & Communications Integration Center (NCCIC): 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the US federal government, intelligence community, and law enforcement. The NCCIC shares information among the public and private sectors to provide greater understanding of cybersecurity and communications situation awareness of vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

National Infocomm Security Committee (NISC): National platform in Singapore to formulate IT security policies and set strategic directions at the national level.

National Information Security Center (NISC): Japanese department that works with other government departments to design and implement cybersecurity policy, including incident and emergency response measures and common cyber standards and recommendations to improve cyber resilience.

National Infrastructure Protection Plan: A US Department of Homeland Security document outlining how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes.

National Institute of Standards and Technology (NIST): Works with stakeholders to develop a voluntary framework based on existing standards, guidelines, and practices for reducing cyber risks to critical infrastructure.

National Security Agency (NSA): Leads the US Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO).

Network and Information Security (NIS) Directive: Proposed by the European Commission, together with the High Representative of the Union for Foreign Affairs and Security Policy, it aims to ensure that critical infrastructure operators (including financial market infrastructures such as stock exchanges and Central Counterparties) meet appropriate IT security standards, share cyber threat information and notify authorities of any significant incident. It also requires EU countries to exchange information on such incidents and it provides implementation and enforcement responsibilities to sector-specific authorities.

NIS Platform: Public-private partnership among more than 200 members in 18 EU member states which met for the first time in June 2013. It includes representatives from research, academia and various industry sectors, and is divided in three working groups to issue guidance on risk management, information sharing and incident notification.

NIST Framework for Improving Critical Infrastructure Cybersecurity: Guide for firms seeking to develop and enhance their cybersecurity program. The framework is the result of collaboration between industry and government, making it flexible and implementable by private sector organizations of all sizes.

NIST National Vulnerability Database: The US government repository of standards-based vulnerability management data. This data enable automation of vulnerability management, security measurement, and compliance.

Open Web Application Security Project (OWASP): Global non-profit organization focused on informing and educating users on the security risks and solutions associated with computer programming.

Open Web Application Security Project Top Ten: Consensus document that covers what cybercriminals are attacking and is updated every year to reflect the most recent changes.

Payment Processors Information Sharing Council (PPISC): An FS-ISAC council which provides a forum for sharing information about fraud, threats, vulnerabilities and risk mitigation in the payments industry.

Payments Risk Council (PRC): An FS-ISAC council which shares payment risk information for ACH, checks and wire payments as well as best practices to mitigate payment risk.

Phishing: Attempt to trick individuals into disclosing passwords, identity information and payment card credentials that would allow attackers to commit fraud.

Presidential Policy Directive (PPD-21) Critical Infrastructure Security and Resilience: Focuses on ways to evaluate and build on existing critical infrastructure public-private partnerships and identify baseline data that will enable the government to more efficiently exchange information and intelligence.

Regulation Systems Compliance and Integrity (Reg SCI): Regulation proposed by the Securities and Exchange Commission that would apply to certain self-regulatory organizations. (including registered clearing agencies), alternative trading systems (ATSs), plan processors, and exempt clearing agencies subject to the Commission's Automation Review Policy (collectively, "SCI entities"), and would require these SCI entities to comply with requirements with respect to their automated systems that support the performance of their regulated activities.

SANS Institute: A private US company that specializes in information security and cybersecurity training.

SANS Institute's Critical Security Controls: A listing of actionable products, processes, architectures and services that have demonstrated real world effectiveness against cyber threats.

Sector Specific Agencies (SSAs): The Presidential Policy Directive-21: Critical Infrastructure Security and Resilience, signed in February 2013, assigns a federal agency, known as an SSA, to lead a collaborative process for critical infrastructure protection within each of the 16 critical infrastructure sectors. In the case of the financial services sectors, the US Department of Treasury functions as the SSA.

Securities and Exchange Commission (SEC): The primary regulator of the US securities markets. The SEC works closely with many other institutions, including Congress, other federal departments and agencies, the self-regulatory organizations, state securities regulators, and various private sector organizations in pursuing a number of cybersecurity initiatives, such as Reg SCI.

Securities Industry and Financial Markets Association (SIFMA): Part of FSSCC's leadership, a US industry trade group representing securities firms, banks, and asset management companies. SIFMA was formed in November 2006 from the merger of the Bond Market Association and the Securities Industry Association.

Security Content Automation Protocol (SCAP): A suite of specifications for organizing, expressing, and measuring security-related information in standardized ways, as well as related reference data such as unique identifiers for vulnerabilities.

Soltra: Joint venture between DTCC and FS-ISAC to develop and distribute a software application and network for the automated sharing of security intelligence to protect critical infrastructures.

Structured Threat Information eXpression (STIX): A collaborative effort to define and develop a standardized language to represent structured cyber threat information. The STIX language conveys a full range of potential cyber threat information that is fully expressive, flexible, automatable and as human-readable as possible.

System Hygiene: Basic practices aimed at improving cybersecurity, such as staying current on patches, configurations and software updates on IT systems.

Systemically Important Financial Market Utilities (SIFMUs): Entities whose failure or disruption could threaten the stability of the US financial system. To date, eight entities in the United States have been officially designated SIFMUs by the Financial Stability Oversight Council.

Trusted Automated eXchange of Indicator Information (TAXII): The main transport mechanism for cyber threat information represented as STIX. Through the use of TAXII services, organizations can share cyber threat information in a secure and automated manner.

US Computer Emergency Response Team (US-CERT): Part of US Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC). US-CERT is responsible for analyzing and reducing cyber threats, vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

US Department of Homeland Security (DHS): A cabinet department of the US government, the DHS is designated as the Sector Specific Agency for several of the US' critical infrastructure sectors.

US Department of Treasury: Executive agency responsible for promoting economic prosperity and ensuring the financial security of the United States. The Treasury is designated as the Sector Specific Agency for the financial services sector.

US Secret Service Electronic Crimes Task Force: Brings together federal, state and local law enforcement, prosecutors, private industry and academia. The common purpose is the prevention, detection, mitigation and aggressive investigation of attacks on the nation's financial and critical infrastructures.

About DTCC

With over 40 years of experience, DTCC is the premier post-trade market infrastructure for the global financial services industry. From operating facilities, data centers and offices in 15 countries, DTCC, through its subsidiaries, automates, centralizes, and standardizes the post-trade processing of financial transactions, mitigating risk, increasing transparency and driving efficiency for thousands of broker/dealers, custodian banks and asset managers worldwide. User owned and industry governed, the firm simplifies the complexities of clearing, settlement, asset servicing, data management and information services across asset classes, bringing increased security and soundness to the financial markets. In 2013, DTCC's subsidiaries processed securities transactions valued at approximately US$1.6 quadrillion. Its depository provides custody and asset servicing for securities issues from 139 countries and territories valued at US$43 trillion. DTCC's global trade repository processes tens of millions of submissions per week.

To learn more, please visit www.dtcc.com or follow us on Twitter @The_DTCC.

This description is for informational purposes. This Service is governed by applicable Rules, Procedures, and Service Guides for each DTCC subsidiary, which contain the full terms, conditions and limitations applicable to this Service. We may provide you with additional information about our products and services from time to time. If at any time you wish to be removed from our distribution list, please send an email to PrivacyOffice@dtcc.com.

To learn about career opportunities at DTCC, please go to dtcc.com/careers.

This paper is available electronically at www.dtcc.com.