Operating within the Threatscape: Understanding the impact of an evolving threat to the Federal Reserve's Information Security, assessing the costs, and implementing solutions

A new form of warfare is being waged upon government organizations. It is more stealthy – more malevolent than a military surgical strike conducted under cover of darkness. It is potentially more destructive than a surprise, frontal attack on a government brick-and-mortar institution. It can strike from anywhere in the world, disguising itself as an important spreadsheet or embedding itself within your network after being planted by an unsuspecting employee answering an e-mail, or plugging in an un-credentialed device. The malware could be a worm that mutates then replicates; or it could be a "logic bomb" pouncing immediately, or perhaps waiting weeks, months or even a year, to swiftly and silently destroy all of the data on your network.

It is real, and it has already struck with amazing ferocity and effectiveness across the digital landscape.

(Sidebar)
A breach occurred when previously undetectable "back doors" were discovered, providing Chinese hackers with access to classified data at the highest echelons within the Department. The source was traced to fake Cisco routers manufactured in China, which had been purchased by our military at a cost of $75 million, through normal channels. Cisco has long outsourced a good portion of their manufacturing to China. However, these routers were designed to allow complete network access to the hackers. The ramifications for the Fed: altered router chips that can mimic normal behavior may be allowing unfettered access to critical financial information, compromising our nation's infrastructure and financial stability.

Sources: Ponemon Institute Report, *FBI Confidential*

Evolution of the Cyber Threat
The nature, severity and increasing frequency of the attacks have resulted in a focused effort given to researching the trend, its intricacies, weak links and the cost of cyber attacks on government and other large entities. From the analysis a new culture has emerged; it is a fact that we rely upon our Information Systems to provide critical functions in every government space. We at the Federal Reserve do not take lightly the risks inherent in this new culture. On the contrary, it is incumbent upon us to be more diligent than ever before in educating ourselves, to a person, regarding the existent cyber threat. In addition, we must become more vigilant in our daily activities, and adapt to the maximum degree in order to protect ourselves from the Information Security risks within our infrastructure.

The landscape of this Information Security risk is evolving. It is neither static nor local in scope; it could be said that the threat never sleeps. Therefore, growing concern is well-founded over any aspect of cyber threats which exploit the vulnerabilities of our assets, which assets are essential to the economy and well-being of American citizens. Of course, these same threats to our organization potentially impact the world at large, since the Fed's

influence and reputation within the world of finance is significant. In today's parlance, it is widely referred to as the *Threatscape*.

The Complexity and Relentlessness of the Threatscape

The cyber criminals who wage such extraordinary, vicious attacks are becoming far more intelligent and clever than ever before. Hackers are not only computer scientists, but con artists who artfully craft ways of reeling in users through social engineering. Hackers have stolen tens of millions of dollars from major institutions, wiped out entire Information Systems and leaked top secret government data to the public and nation states, in strategically targeted, well-orchestrated cyber attacks.

Taking seriously the prospect of cyber threats at every level of our organization, two things remain true:

- Any device that is computer-controlled and networked is vulnerable to hacking.
- Secondly, to be sure, what we have been doing up to the present to shore up our Information Security has been sufficient to ward off cyber attacks thus far. However, we are not only facing an unseen enemy, but one who has grown more cunning, more resourceful and in many cases, well-funded. The hackers' stealth and leverage are not to our advantage, and seemingly impenetrable government organizations, such as the Department of Defense and the CIA, have already been hacked.

The cost of cyber crime upon any government organization cannot be realistically weighed or understated. That is why even the most sophisticated, well-guarded systems of ours cannot be taken for granted. We are faced with a nemesis that has taken a leap in technology and cleverness, at the very least. With this in mind, we can no longer afford to be comfortable with the status quo regarding our levels of vigilance and Information Security. Now we must redouble our efforts, hone our awareness and educate ourselves to a host of potential problems and work on their solutions together. A suiting truism for us at the Federal Reserve is that cyber security trumps cyber convenience.

(Sidebar)

The most sophisticated piece of malware ever engineered, and the weapon of the first cyber war in history, may have been initiated with something as simple as a USB flash drive. Attacking the computers of Iran's Bushehr nuclear facility, the worm exploits four, previously unknown "Day Zero" vulnerabilities in the Windows OS. Once inside, it hid its tracks, infected some 30,000 IP addresses in Iran and eventually spread to computers in India and Indonesia. It is spreading fast and has mutated three times, designed exclusively to infiltrate operational facilities and initiate crippling responses coupled with mass transferal of data to foreign countries. It has been stated that the resources needed to stage this attack point to a nation state. The ramifications for the Federal Reserve are apparent: if a worm of this complexity and power could be developed to infect an operational facility, a variant could be written to include infection and propagation within the financial space.

Source: University of Dayton Research Report

Why you are reading this white paper
This white paper has been developed in view of each of the foregoing, significant premises, and illustrates why it is imperative that we all be proactive in our approach to the Threatscape. This resource is being distributed among top-level executives within the Federal Reserve to help underscore the magnitude of the Threatscape, and has been engineered in order to allow us to become better prepared in meeting and mitigating the evolving dangers ahead, from the standpoint of cyber security.

What you will learn
As you study this document you will gain a far greater field of vision within the Threatscape as it impacts the Federal Reserve, both presently and for the future. The information provided within these pages will help you to recognize the multiple threats and points of attack we all face at this moment. You will gain the insight necessary to conceptualize the cost of IT security in terms of the needed investment of time and resources.

You will learn about the types of threats that currently exist within the Threatscape, and how other government entities responded to recent cyber attacks “on their own soil.” You will also learn about the defense measures and best practices these organization implemented to mitigate the threats.

You and your constituencies will grow in the understanding that we at the Federal Reserve are a target for the same types of cyber attacks. On the same hand, you will nonetheless grow in the understanding that we need to be ahead of other entities because of our high profile and crucial role in the American economic landscape.

Armed with the information and background provided, you will gain a vision for the future Information Security strategy that incorporates security solutions technology, business practices, processes and resources, plus the all-important culture of security that will help protect the critical infrastructure of the Federal Reserve.

Finally, you will be provided with a list of additional resources and from Federal Reserve Information Security experts in order to gain a deeper level of information on the Threatscape.

Operating within the Threatscape

The evolving world of information security risk and its impact on the Federal Reserve

Everyone understands the critical importance of information security to the Federal Reserve, our critical infrastructure, and our role in setting monetary policy. However, the landscape of information security has changed dramatically, and the threats we face today go far beyond anything we have encountered before.

At this moment, we all work amid a constantly evolving Threatscape. At risk are our most vital information and our reputation. This is the reality of the new landscape of information security risks.

The Threatscape is highly sophisticated, constantly evolving, and the enemy is truly relentless and often unseen. As we strengthen our defenses, cyber criminals shift their attack strategies. They wait for the optimal moment and choose the most vulnerable point to strike.

Even more alarming, the Threatscape is already within our inner circle, searching for any unsecured entry point.

Like the internal project status email from a colleague that appears legitimate. But when it is opened, the email contains a virus that has bypassed the firewall and systematically shuts down the network. Or the flash drive that allows a manager to work from home. But when it is plugged in back at the office, the flash drive downloads a “logic bomb” that waits for months to destroy vital data.

Clearly, operating within the Threatscape demands more than vigilance and standard technology defenses. It requires an IS strategy that incorporates innovative security solutions technology, renewed business practices, more focused IS processes and resources and a heightened culture of security.

No single defense measure alone is enough. It also requires an investment, including resources, time and the dedication of every individual in order to protect the critical infrastructure of the Federal Reserve in this ever-evolving Threatscape.

Identifying the threats at every workstream level

Experts who have analyzed the evolving, relentless, stealthy and sophisticated cyber threat have also determined that constant vigilance is required at every workstream level. That is, across every form of access, every IT area and by every person. To simplify the process of vigilance and see this threat with new eyes, let’s consider each of the different workstream levels and the potential vulnerabilities they present.

The Identity Threatscape

“The security gap is end users,” says Kevin Mandia, Chief Executive of security firm Mandiant Corp. The majority of security breaches currently being investigated by his company involve hackers who gained access to company networks by exploiting well-intentioned employees.

The gateway for threat entry often lies with

- ✔ misused or neglected logins
- ✔ usernames and passwords
- ✔ cards
- ✔ tokens
- ✔ databases
- ✔ web-based access
- ✔ email; webmail

In fact, Web-based threats occur every 4.5 seconds in today's cyber threat landscape. Additionally, with regard to identity theft, employees are being hacked more than computers.

The lurking threat targets and exploits complacent users through the use of social engineering, when strict web navigation and email policies are relaxed or not in use. This trend points mainly to a low level of enforced Acceptable Use Policies (AUPs) with regard to:

- **Email spam and unobserved white listing practices.** One large piece of malware was hidden within an innocent-looking spreadsheet, attached to an email. The offending email, originally dumped into a spam folder, was retrieved due to the level of user curiosity it generated, and subsequently infected an entire network.
- **Phishing and spear phishing attacks** derived from social engineering tactics.
- **Bots and rootkits** that can allow worms, trojans, logic bombs and other viruses, pose the greatest risk.
- **Password policies** that stress password strength, as well as other regulatory requirements regarding passwords, may tax users and drive behavior that reduces security.
- **Out-of-date software vulnerabilities analysis** on the part of the users can allow constantly evolving threats to spread.
- **Available software patches** that may not be applied in a timely manner, exposing vulnerabilities.

The Workstation Threatscape

The significance of threats at this level is based on research and findings that point to the individual workstation as a frequent entry point for advanced cyber attacks. As can be seen, increased vigilance and common sense become a theme within the new culture of awareness: these threats do the most damage when individual awareness is low and prevention is overlooked.

- Unrestricted or less-restricted use of un-credentialed devices and removable media.
- Included within this list would be mobile devices, minicomputers and all other processor-driven devices that connect via USB at the workstation or server. In many cases, the line has become blurred between the personal and professional use of

technology. As a result, threats to sensitive data and Information Systems have become myriad. A new reality is that un-credentialed devices are the second most critical players in the Threatscape.

- If the configuration of a workstation or set of workstations can create a path to critical applications and data sources, an increased risk for infection to the whole system likely exists.
- Lateral movement from one workstation to another presents another significant threat. When AUPs, as well as an increased level of awareness and vigilance, are not being observed, the possibility for infecting the system can increase exponentially with a single movement.
- Software companies often play catch-up with cyber criminals. Whether an AUP has not been enforced or an Intrusion Prevention System (IPS) has not been put in place, a higher probability of infection will exist at the workstation level.

The Network Level

Patiently choreographed, well-thought-out, well-orchestrated cyber attacks at the network level, have become the new norm. They are typically aimed at high-profile agencies and institutions, often resulting in Total Denial of Service (TDoS). Cyber criminals are usually skilled and well-funded; however, another type of cyber criminal, known as the “Hacktavist,” attacks just to prove a point. Either one can present a maximum threat.

Threats at the network level may stem from one or more of the following:

- Routers and other network hardware may not be legitimate. In fact, such fake equipment has been designed with modified chips that transfer sensitive data to provide hackers or nation states perpetrating the cyber crimes with highly valued, sensitive information. Ultimately, a crime of this magnitude could jeopardize the safety and stability of an offended nation or governmental body.
- Inadequate protection within firewall gaps. Some firewall applications may allow seemingly innocent applications to “pass through” when they may be infected. Examples of recent exploits occurred through multiple Windows zero-day flaws in popular software, including Adobe Flash, Reader and Acrobat.
- Less-secure wireless LAN protocols, possibly driven by a perceived lower level of threat or vulnerabilities assessment, inattention of IT staff, or less-complex Internet use in a given area at the network level.
- An “inside job,” whereby malware can be planted into the network by a malicious employee or contractor. Anyone with an axe to grind may be the weak link in the IS chain. A comfortable level of screening or security within a facility can allow an employee with a data card or USB drive to penetrate an entire network within seconds, similar to what recently occurred in Iran with the Stuxnet worm.
- Low web security gateway functionality in operational enterprise software and network applications. Examples include anti-malware, URL and content filtering.
- Increased threats due to less-robust access measures. An example would be if the system within the network allows a “replay” of the user’s active directory password.

The Server Threatscape

Server threats are extensive due primarily to the fact that most of the problems affecting networks also apply to servers.

- Criminally planted subassemblies or chips within servers can be specially designed and modified to allow hackers to gain unauthorized entry into a network.
- Lack of vigilance on the part of dedicated IT personnel can compromise information security if access to servers is not strictly monitored or otherwise controlled.
- The simple act of leaving servers un-patched and running out-of-date antivirus software exposes vulnerabilities to the entire system.
- Exploiting firewall vulnerabilities allows malware to penetrate and propagate.
- Malicious intrusion from the inside into un-patched, unsecured servers, opening up the IS to cyber espionage.

The Visibility Threatscape

Visibility threats now need to be examined using both “micro and macro” monitoring, prevention and detection approaches.

- Getting users to think critically about online security in terms of lessons they have already learned on an individual basis, helps. There are no “band-aid” solutions for specific issues.
- Training and education, combined with a new culture of awareness and vigilance, are far easier measures to implement than enterprise software solutions and fixes to infected networks.
- Every individual matters within the Threatscape and, properly advised and trained, makes a “majority of one” difference in the security of the organization.
- “One-size” enterprise monitoring does not fit every need. Methods such as signature-based monitoring create exposure that can be lessened by business-centric monitoring.

Practices and policies must adapt to the changing Threatscape

In view of the baseline imperative for a stronger culture of awareness and more proactive stance within the IT community, the question remains: How to protect Information Systems from hacking and exploitation? Although specific solutions will be multifaceted and need to fit the size, scope and components of the organization’s Information System, the following key aspects present the best place to begin in answering to this question:

- Begin questioning what was never questioned before within the purview of the IS landscape.
- Employ an integrated approach – a graded system with checks and balances, coupled with comprehensive IS architectures and deployment strategies.
    - The State Department has pioneered an approach to IS that makes it easier for managers to identify trouble spots, prioritize them and employ sure, expedient repairs.
- “Leave no stone unturned.” All systems, all users, and all IT personnel need to come under a heightened level of scrutiny.

- Along with the understanding that a need exists for comprehensive training programs coupled with enterprise deployment of Security Incident & Event Management (SIEM), policies must adapt to meet the Threatscape head on.
    - Business workflows may need to be reengineered.
    - Technologies will most likely need to be designed or redesigned with IS as a cornerstone.
    - More strict use and user-screening policies within a larger AUP framework.

END OF SAMPLE