

Remarks by Donald F. Donahue
FS-ISAC Spring Member Meeting: Keynote Address
May 5, 2009
The Public-Private Partnership and Supply Chain Resilience

Good morning, everyone. I'm very pleased to be here at the FS/ISAC spring conference. I might grumble that Jim Routh pulled security rank to cajole me into being your keynote speaker, but it really didn't take much arm-twisting. Resilience in the financial services infrastructure is not only personally important to me, but critical to the industry itself, and I'm delighted to have the opportunity this morning to speak to you.

Escalating Threats

The assaults on the nation's cyber infrastructure have escalated, with exponential increases in both the sophistication of the attacks and the threats they pose to our industry and our nation. As we all know, the malefactors have long since gone beyond the "I'm-smarter-than-you" kids who crash computers and delete files. Today's cyber enemies routinely steal and market passwords and financial information; they've breached well-defended national defense systems; they've infiltrated the very computers that control the power grid in other countries. As sophisticated as the cyber criminal class has become, it's clear that we're also up against nation-state opponents, with the even deeper levels of capabilities they have to be assumed to have.

With all the recent high-profile cyber security incidents, there's no question that we need to make qualitative changes in our strategies to protect the supply chain supporting the financial services infrastructure. And a key foundation element of our strategies to cope with these increasing threats must be building and reinforcing a collaborative approach to integrating the public and private efforts in this space. We need a true "give and take" on what both sides know or suspect regarding vulnerabilities; we need a true public/private partnership on how we go about ensuring the bullet-proof resilience of the nation's cyber infrastructure.

Only that type of partnership and collaboration can form a strong basis for an ongoing action plan to create and implement the protections we must have.

We're here today to encourage that partnership, to share our experience — and to listen and learn from others.

DTCC's Experience

The industry puts its trust in DTCC to clear and settle more than \$1.88 quadrillion annually in securities transactions, and the stability of the financial system depends on our ability to deliver. What we do is critical to the integrity of the financial markets, and "Trust" is literally our middle name. We are the largest financial services post-trade infrastructure organization in the world, and from our central vantage point, we provide services that cover just about every asset class.

At its core, DTCC is a huge data processing business, involving the safe transfer of billions of dollars in securities and funds under tight deadlines every day. For us, resilience in our infrastructure and software security is not a 'nice to have.' It is an absolute business imperative.

With that central role in the securities industry and the sheer values and volumes of transactions we process—

roughly the equivalent of the entire U.S. GDP every three days — you can believe that the bad guys out there are constantly testing our doors, jiggling the locks, looking for the tiniest crack in our security. At best, they're merely in it for the challenge, to boast about their prowess. At worst, however, we face organized cyber enemies who are hell-bent on positioning themselves to bring down the entire U.S. financial services system.

We don't kid ourselves about the seriousness of the threat they pose. These enemies are well-organized, well-funded, malicious — and global. They're every bit as technologically advanced as the most sophisticated software company. And they are fast, very flexible, and very difficult to track and apprehend. Their intent to penetrate the supply chain exploiting whatever vulnerabilities that may exist is very clear.

I can still sleep relatively well at night, however, because DTCC has invested in the implementation of mature governance practices for vulnerability management throughout our supply chain. I can sleep because, through our work on our comprehensive software security program, we have effectively broadened our definition of "supply chain" beyond just the end product — software and hardware — that customers use to interact with our services.

When we think of the technology supply chain at DTCC, we look at the entire lifecycle — from its creation to its retirement. We look at it from:

- the originating point of manufacture and coding — in other words, where it is manufactured, and by whom,
- the access controls throughout its development and delivery, and finally,
- servicing this end product of hardware or software.

For the software and the hardware that customers actually use, that supply chain incorporates four separate channels:

1. software developed internally
2. software outsourced to 3rd party service providers
3. software purchased from vendors
4. hardware and appliances

Weaknesses in this supply chain can be very real, especially if we are complacent about them. So protecting the resilience of the supply chain requires understanding our existing practices and controls, staying educated as new "best practices" evolve in the industry, and constantly applying this understanding and awareness of new practices to improve our own practices and controls using every lever available to us — for example, through leveraging our procurement processes. This requirement pertains whether we're talking about software we build or buy; services we acquire; or hardware we procure.

In terms of supply chain resilience, the adage has never been truer: no chain is stronger than its weakest link. Unfortunately, we see the potential for several weak links, any of which can snap the entire supply chain.

I'm going to talk a bit about a few of these weak links, and I think you'll quickly see why they're literally quite a handful to manage.

Weak Link #1: Insider Threat

The first weak link — and, truthfully, the one that does keep me up at night — is the insider threat.

Our vulnerability to ill-intentioned insiders remains a persistent problem. Our computer, software, and network designers; implementers, coders, installers, and maintainers all have access to our systems, know how they work, and know their weak points. So they certainly have opportunity; God forbid they get a motive. The vulnerabilities "insiders" feel during an economic downturn — certainly the environment we're all living

through— raises the stakes here; an insider who feels he’s been mistreated because of, say, a salary freeze or who feels threatened by the potential of a lay-off could certainly get the idea of acting to cause major damage to any one of us.

This is a risk that we all understand, and we know that, at the end of the day we have to trust our people, and therefore need to know that they are trustworthy. This is the idea behind background validations, lie detector tests, personality profiling, and limiting certain jobs to people from areas where these kinds of checks can be done. As all of our firms increasingly outsource key technology operations to other areas of the globe, however, the “insider” risks have morphed. Outsourcing critical pieces of code development to countries that harbor known cyber enemies – essentially making their people quasi-“insiders” in your technology operations – involves risks that should make us all nervous. Background checks become even more important in this context, although, as you know, they’re also even more challenging in many locations to which we’re now outsourcing our technology work.

I personally believe that this area offers one possibility for a fruitful collaboration between the public and private sectors. Clearly our public sector partners have access to much more information about our cyber enemies. How can we work with them to have our background checks enriched through leveraging this heightened knowledge in our screening processes? Not a simple issue, but one we absolutely have to think about and come up with a viable answer to – if heightened screening procedures can be used for casino employees in Las Vegas and Atlantic City, as they are, we need to think about how they can be deployed to reassure us about our trusted insiders.

Insiders also, of course, don’t have to be malicious to create risks for us, and in future this will be increasingly the case, as my experience with another technology operation I’m responsible for illustrates. I have an “insider” in that technology environment who is very technology savvy, used to routinely multi-tasking with a variety of technology systems, and frequently makes technology decisions that pose very new risks for me as her supervisor – perhaps I should say “alleged supervisor.” I am, of course, talking about my 15-year-old daughter, who, like virtually all of her contemporaries, has been weaned on the Internet and has a technology-based lifestyle that is qualitatively different from her elders – someone who was “born digital,” in the title of a recent book. In the coming years, we will all be ushering this generation into corporate America, and many of them will unquestionably use their technical savvy to create holes in the very controls that protect our most vital technology assets simply in very natural pursuit of their “multi-tasking” lifestyle.

Today, most financial firms block access to social network sites and have no plans to change policies; most do so not for security reasons but for productivity reasons. An issue we’ll confront going forward is how we balance this qualitative transformation in how our newest employees are used to working and living with the clear information security vulnerabilities it presents. So the “insider threat” issue is about to get even more interesting!

Weak Link #2: Software Vulnerabilities

Almost 90 percent of reported security incidents result from exploiting defects in the software we use, so ensuring the integrity of that software is critical to protecting the infrastructure and reducing the overall risk of cyber attacks. Recently, technology executives at DTCC, as well as those at Adobe, EMC, Google and Microsoft, among others, participated in a benchmarking report on software security from Cigital and Fortify Software called "Building Security in Maturity Model (BSIMM)." I am extremely proud that DTCC’s four-year-old software security program was recognized by the authors of the study, published in March, as one of the most advanced in the world.

The BSIMM report is the first-ever scientific observation of common domains and activities for developing an enterprise-wide software security initiative. It provides real-world insight into how organizations — like ours

— successfully build security into software, to mitigate the business risk associated with insecure applications. You'll hear a lot more about it from Dr. Gary McGraw and Roger Thornton tomorrow.

What differentiates the model discussed in the study is the shift in the security paradigm it represents. We're not simply playing catch up or a wild game of "whack-a-mole" with patch management. Instead, we pay attention to creating more effective software assurance even as we're writing code.

For example, DTCC's developers have now been conditioned to "front-end load" by rigorously checking for vulnerabilities early in the code development lifecycle, rather than relying on penetration testing at the end and fixing defects after the code is in production. They leverage a pre-established security application architecture that addresses the authentication and entitlement management design issues, enabling them to focus on building new functionality. This has significant economic benefit in terms of productivity achieved (about 13%)— and risk mitigation for customers.

We come by this disciplined approach from the rigors of being the only U.S. financial services organization to have a CMMI Level 3 rating across our entire Applications Development and Maintenance enterprise. Over 70 security mavens are expressly trained in software security, 12 of whom are GSSP-certified by SANS. You'll hear more about SANS certification from Alan Paller and Mason Brown.

But, of course, software security isn't a one-time event. These issues are present every time we enhance or upgrade our systems, and every time we install patches or other fixes to third-party products we use — and top-notch efforts in one part of the cycle can be undone by something that happens downstream. A situation we had last week illustrates the problem. Metrics we report to our Board include measures of information security incidents, and last week I had the pleasure of explaining why we had in one month 18 violations of security standards on our server configuration settings. The answer? We installed 18 patches that reinstated security violations due to vendor settings incorporated into the patches. We had asked these vendors to permit us to change their patch installation procedures to prevent security exposures and comply with our security settings; their answer was that if we changed the patch installation procedures, they would no longer support the software. We clearly can do better on these kinds of things, in part by understanding how we can leverage the buying power within our firms to achieve better "out of the box" security settings. John Gilligan will be talking about this in a few moments.

Weak Link #3: Hardware Components

In securing the supply chain, we also have to look at the physical hardware that we plug in to the network. This is the third potential weak link — hardware component security.

Where was the hardware manufactured, and by whom? If it's a "white label" OEM product, could it possibly be counterfeit? This might seem the height of paranoia, but note that, for example, the FBI has been conducting a multiyear investigation into counterfeit Cisco routers. It's not a big leap in logic to see how this kind of questionable hardware could provide a backdoor into otherwise secured systems.

At the consumer level, there have been several high-profile incidents over the past year of computer parts or devices being sold with malware already installed. For example, last Christmas, consumers bought thousands of digital photo frames, GPS devices and USB memory sticks all pre-loaded with malware that would infiltrate and infect their computers. Hardware testing for security vulnerabilities is in its infancy and must improve to meet industry requirements. Another issue for us all to focus on, especially our vendors —how to improve our practices for preventing hardware sabotage.

At DTCC, I think we do a pretty good job at enforcing security standards and settings, changing default passwords, and addressing software security issues. But we, like you, have to be equally vigilant about securing

and protecting the hardware we use. The financial sector has to embrace the same kind of thoroughness and discipline about hardware security that we already see becoming prevalent in the sector's software security practices.

Weak Link #4: The IT “Monoculture”

The reality is that all of our firms have information technology environments that are largely similar. Our integration with, and interdependence on each other is reflected in the reality that we rely as well on the same software packages, by and large; the same hardware vendors; and the same networks to interact with each other, particularly the open networks. This brings us to the fourth weak link in our supply chain, the risk and vulnerabilities posed by the sector’s concentration around particular software and hardware.

Through FS/ISAC, the financial sector is doing an increasingly better job at identifying the concentration risks and vulnerabilities. The Supply Chain Working Group toolkit that Jim referenced a moment ago – which I understand you’ll be discussing further later in the conference – is a perfect example of this. However, our sector is extremely reliant on other sectors that do not have the same level of awareness, regulation or even organization, and so it’s pretty obvious that we can’t do this alone.

A lot has been said through the years about buying power as a means to improve the security and resilience of the technologies we rely upon. Just think what would happen if every organization attending this conference today were to specify and implement an industry-standard set of uniform security requirements for all commercially purchased technology – turning the essential similarity of our environments from a potential weakness to a source of very real strength. Leveraging our industry scale would send a very clear message to the software providers that they can no longer rely on assumptions that they know what our security needs are, and that actual demonstration of controls to eliminate security vulnerabilities in the software development process is both essential – and required.

Not surprisingly, the power of procurement has amazing leverage in the marketplace. A key theme of this conference will be how, together, we can improve the governance and controls in place for our procurement of software, services and eventually even hardware.

Weak Link #5: Access Controls

And finally, the fifth weak link in the supply chain is access controls. No matter how proactive your information security team is in building a hardcore, secure system, running penetration tests, and continually modifying and fortifying the armor, firms can become blind to the obvious: the risk in concentrating access controls. The recent CheckFree exploit – that we’ll be discussing in one of the breakout sessions later this morning – provides a clear example of how access controls at a supplier were compromised. This incident could have been a lot worse, and, if they can do it to one financial institution, we have to be ever-vigilant that they can do it to other financial institutions.

The Public-Private Partnership

Some of you may have played a board game called RISK. It’s actually a good metaphor for what we’re up against. In the game of RISK, players control armies to capture territories from other players. The goal of the game is world domination. The outcomes of battles are decided by rolling dice. In the game, attackers have more dice. Just as in the real world, they have the advantage.

Now, while alliances do not exist in the official rules of the game, if you’ve ever played a knock-down, drag-out, all-night game of RISK, you know that players often form unofficial treaties to safeguard themselves from attacks, or to eliminate a player who has grown too strong. Alliance-making can be one of the most important elements of the game.

If we're going to win this fight against our sophisticated cyber opponents – now, more than ever, we need such an alliance between the public and private sectors.

As chairman of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security a few years ago, I saw how our group of more than 30 private-sector firms and financial trade associations formed just such an alliance with the public sector – the Treasury Department and the regulatory community – to help reinforce the financial services sector's resilience against terrorist attacks and other threats to the nation's financial infrastructure. Our mandate was to build and improve these exact kinds of public-private partnerships, to facilitate knowledge-sharing and the timely dissemination of critical information among all sector constituencies.

There are multiple pieces to the infrastructure protection puzzle, and no one of us holds all of them. We each have pieces of relevant information and knowledge. Some of those pieces are held by the private sector and others by the public sector. The pieces we each hold individually may not seem meaningful in themselves, but when many of them are brought together, patterns become clear, sequences come into focus, and the whole picture starts to take shape.

Nowhere is that more true than in the context of the cyber threats and the cyber security issues. Nowhere is it more true that the public sector and the private sector need to form a relationship that permits us, as partners and collaborators, to put our pieces together to frame a clearer picture.

In the past year, there have been significant improvements in information sharing activities. In fact, this conference itself is an excellent example of the power of sharing information. All of us will benefit enormously from the information shared, which will improve everyone's controls for security and protection.

As we talk through how we should seek to respond to these new threats, I think it is imperative that we remember what has been the key to our success in infrastructure protection efforts thus far – willingness on both sides to work collaboratively and cooperatively to formulate strong responses to these challenges.

I'd go further. Given the nature of the threat, as in the game of RISK our efforts to respond will be fatally weakened if we don't work together. And I don't need to remind anyone here: this is not a game.