

Why is messaging security key to communications and National Security?

"Cyber" and communications system form the nexus of all of our critical infrastructures and key resources.

First, Messaging includes the entire spectrum from email, to text messaging, to instant messaging, to Voice-Over-IP (VoIP), comprising most electronic communication today. The ability to block malicious content from entry and guard protected content from exit is the enabler of high-speed business transactions from both an economic and an infrastructure protection perspective. This protection must extend to every entry and exit point – including email gateways, web gateways, phone handsets and PDAs. All of the castle doors need a guard.

Secondly, electronic messaging is the medium upon which many emergency/first responders and other infrastructure protection communications rely. A failure in the safety or availability of any of these systems can cause delayed response or other harmful results.

How do you view your role in infrastructure protection?

I view my role as one who learns and one who educates, and I have two very separate positions, both in the infrastructure protection space:

I am a private sector employee of Secure Computing / CipherTrust. My role from a research perspective is focused on helping to develop, explain, and protect our new technology/intellectual property. This includes understanding how our products work, and the effect that our messaging gateway protection and intelligence has in the big picture of critical infrastructure protection. I work with my CipherTrust colleagues, customers, and anyone in the chain from whiteboard to deployment needed in order to best understand ways in which they can better protect their networks.

As a volunteer position, I am the Chairman of the Board of Directors of the InfraGard National Members Alliance (INMA). My key responsibility is to enhance the Boards ability to enable all 85 of our local InfraGard chapters to build trusted cross-sector and cross-agency relationships within their local communities. Most of my focus is on building and maintaining the external relationships (in addition to our core trusted relationship with the FBI) for the INMA with other agencies and organizations such as DHS, the U.S. Chamber of Commerce, ASIS, ISSA, Sector Coordinating Councils, the Department of Commerce, and many others. Our local chapters use these National relationships to build their own, local trust relationships as well as to obtain information and subject matter expertise from the Federal level.

Among what I learn from my work with Secure Computing is how customers react to technology in various circumstances, and where value is best provided from communications security. From

this, I can better understand how to engage other in the private sector to embrace security and infrastructure protection wearing my volunteer InfraGard hat.

I have learned from both positions that I do not require a lot of sleep.

Why is “information sharing” broken?

I am including some thoughts in the next 2 questions from a white paper by my colleague Rob Schmidt, who serves as the President of the INMA, as I narrow the faults of information sharing into these points:

- 1) To date, the concept of a shared response has been forgotten or neglected in favor of information sharing between government and industry. To achieve an effective risk mitigation strategy, we must correct this mistake.
- 2) The “Information Sharing” model that relies only on technology (email lists or electronic information distribution en masse) is broken.
- 3) The hurdles that impede effective “public-private” information sharing revolve around non-trivial issues of trust. Public and private have different goals and both sides need to receive the desired value before cooperation is truly successful.
- 4) The private sector does not trust the government to safeguard its secrets regarding infrastructure protection successes or failures. Current efforts to reassure the private sector have been ineffective.
- 5) “Actionable Information” is the only information that is important to decision makers in private industry, and is the only information that, if shared by the government, will build trust with industry.
- 6) Actionable information is only shared by individuals who:
 - a) Trust each other;
 - b) Have a stake in each other’s wellbeing; and/or,

- c) Are united by a common adversary.

- 7) Industry and government need actionable information generated by trusted individuals.

What is a better direction toward a solution to the problems currently existing in “information sharing?”

The government must enable the private sector to participate in its own defense.

- 1) Move technology and knowledge from government (DoD, etc.) into the private sector market place.

- 2) Practice the concept of a “shared response”. This can best be achieved by expanding the scale and scope of public-private exercises.

- 3) These exercises must go beyond “table-tops”. They must stress more than communication and coordination paths. They must force shared response decisions, based on actionable information shared between government and industry.

- 4) Support programs that bring together and establish trust (on an individual, personal basis) between the private sector and government (the FBI’s InfraGard program; DHS’s Protective Security Advisor (PSA) program, etc.).

- 5) Provide resources to organizations that support the exchange of subject matter expertise. For example, if key private sector/companies (such as utilities) were given an allocation of funding to provide the time of some top experts in that infrastructure space as needed, the often conflicting “protection v revenue” issue would be resolved. SMEs could be kept on call and the small part of their time used in knowledge preparation or response provision would not be a financial loss to the organization.

- 6) Over time, increased trusted cooperation will drive a culture shift toward the desire to exchange knowledge across organizations, government agencies and sectors to protect our way of life.

How do we implement the solution -- how can companies effectively share information with government, law enforcement and other companies while still maintaining regulatory compliance and protecting corporate private data and intellectual property?

Companies need to build trust-bases in these three areas - [government](#), [law enforcement](#) and [private sector](#) - with other government and private organizations to enable knowledge exchange and access to subject matter expertise at the local, state and Federal level – before a time of crises. When information and help are needed, those pre-existing relationships transcend competition in the spirit of working together to protect our critical infrastructures. Sharing information is about channeling subject matter expertise to where it is needed, across infrastructures, across organizations. Customer data, corporate data and other protected information need not be exposed. Expertise, for example on the payload of a particular email or on how a power outage in one state might affect energy provision in another, can be shared among trusted conduits. Ironically, such expertise transfer does not breach security – it enhances security.

How can I get involved in critical infrastructure protection and be utilized as an SME?

The quickest way to get involved is to join InfraGard – application is available online at www.infragardmembers.org. Once the FBI approves your membership, you will be sent a survey on your expertise and, upon completion the survey, you will be entered into a National SME matrix available to several government and law enforcement agencies. Also, the National Infrastructure Protection Plan is available from the Department of Homeland Security at www.dhs.gov.

Where can I report cyber attacks/intrusions?

In Atlanta, FBI Cyber Division – 404-679-9000

FBI – www.ic3.gov

U.S. CERT – 888-282-0870

Critical Infrastructure Threats – National Infrastructure Coordinating Center – NICC@dhs.gov or 202-282-9201