From: Robert Zager <Robert.Zager@iconix.com>
Date: Friday, April 5, 2013 7:47 PM
To: cyberframework <cyberframework@nist.gov>
Subject: Developing a Framework to Improve Critical Infrastructure Cybersecurity

To: Diane Honeycutt, National Institute of Standards and Technology
From:James Davidson & Robert Zager, both of Iconix, Inc.
Re: Developing a Framework to Improve Critical Infrastructure Cybersecurity
Date: April 5, 2013

There is no single technology that will encompass the security of all data entering system infrastructure. Differing methodologies and technologies will be needed in separate stages of the data processing cycle.

We are suggesting that the cybersecurity framework recognize the significance of people in this process – with a particular emphasis on the email threat vector. It has now been well-established that the most effective means of introducing malware into data processing systems is through socially engineered emails. Cyber attackers target human email recipients using socially engineered email to disrupt sound decision-making. Dr. Frederick Chang, former NSA Director of Research, observed, "…cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines." The power of this observation was emphasized by the recent Mandiant Report, "APT1: Exposing One of China's Cyber Espionage Units."Mandiant found that:

1. 100% of compromised systems had up to date anti-virus software.
2. 100% of compromises involved stolen credentials.
3. 100% of compromises involved deceptive socially engineered emails.
4. On average, systems were compromised for 416 days before the compromise was detected.

The lesson from Mandiant's report is that the weak link in cybersecurity is the holder of system credentials.Hence, in Advanced Persistent Threats, the first phase of the attack is surveillance of the class of human targets who hold credentials, followed by targeted spearphishing emails at that class of user. Spearphishing email is used to install surreptitious command and control software which then initiates the exploits.

Countering highly targeted socially engineered emails with training is problematic because:

- Socially engineered emails are crafted to avoid suspicion.
- Email processing is driven by perceived relevance, urgency clues and habit (see, Vishwanath et. al, "Why do people get phished?"). These factors are easily exploited by social engineering.

We propose that the cybersecurity framework include the use of visual icons in email as a feedback mechanism to enhance the proactive recognition of reliable data sources. Conceptually, this is akin to "Identification: Friend or Foe," providing simple visual discriminators for improved human decision-making.