Absio®
Take Control of Your Digital World ℠

December 16, 2013

Information Technology Laboratory
ATTN: Adam Sedgwick
National Institute of Standards and Technology
csfcomments@nist.gov

Subject: Absio Corporation's Comments on The Preliminary Cybersecurity Framework

Preamble

The Maginot Line has, for good reason, has become symbolic of (1) strategies doomed by ignoring known problems and (2) fighting today's battle with yesterday's weapons. Absio asserts that the Cybersecurity Framework (CF) as currently envisioned will inevitably result in a cyber Maginot Line, an incomplete strategy that will be all too easy for our enemies to defeat.

The Maginot Line

The Maginot Line was a line of fixed fortifications, weapons, and obstacles that France constructed along its borders with Germany in the 1930s. Its purpose was to deny access through the border in order to provide time for the French army to mobilize and fight the Germans in Belgium.

The Maginot Line strategy was not so much wrong as it was wrongheaded. France's military experts were refighting the last war, basing their plans on the success of fixed defenses in World 1. Their rational was simple: "We know fixed defenses work most of the time. All we need to do is build a lot of them and we'll become impregnable!" They stubbornly adhered to this opinion in spite of the obvious successes of Germany's new strategy, the Blitzkrieg—fast, highly concentrated armor- and air supported attacks specifically designed to penetrate or circumvent fixed defenses. The French military establishment's characterization of the Maginot Line as a work of genius capable on its own of preventing an invasion created a false sense of security. Some in the military disagreed, but the expense of building the Line had absorbed resources needed to purchase mobile defenses. The French military establishment bet nearly everything they had on the Maginot Line and lost spectacularly. Once the Germans outflanked the Line and there was little to stop them. They took France in six weeks.

The Cybersecurity Framework is committing the same strategic error. It states "The Framework relies on **existing standards, guidance, and best practices** to achieve outcomes that can assist organizations in managing their cybersecurity risk" (emphasis added). A plain reading of the Preliminary Framework leads one to believe that full implementation of existing standards, guidance, and best practices will assure the security of the implementer's data. That is not even close to accurate.

It usually takes years to create new controls. Then it takes more years for new controls to go through the standards development and certification process. The less incremental and more revolutionary new controls are the longer standards development takes. The time lag means there will always be (1) vital controls for which standards have been developed, (2) vital controls that are too new for standards to have been developed, and (3) vital controls that have yet to be developed.

To base a defensive strategy solely on number 1, while ignoring numbers 2 and 3 is how Maginot Lines get built.

Examples of Known Gaps

Two examples gaps are (1) data-centric controls and (2) the integration of data-centric controls with environmental controls. Data-centric controls are bound to the data. They are mobile—they go where the data goes. NIST is familiar with data-centric controls and the need for integrating them with controls for which standards have already been developed, but they are not cited in the Framework because they are too new for standards to have been developed. Instead, the Framework only cites environmental controls, that is, controls bound to the environment that contains the data.

Environmental controls include physical controls like tamper-proofing, user authentication, anti-malware software, storage encryption, application whitelisting, firewalls, and many, many more.

Environmental controls are essential but alone they cannot mitigate the insider problem—and data loss is essentially always an insider problem. Whether attackers get inside via a perimeter breach (hacking or phishing, social engineering) or by invitation (Manning, Snowden), it is from the inside that they do their damage.

To illustrate the result of relying solely on the environment controls cited in the Framework, let's walk through an example of current world-class cybersecurity practice using the scenario of provisioning a new notebook computer. The notebook comes out of the box and then you:

- Assign and implement an administrator username and password,
- Encrypt the hard drive,
- Patch the operating system and applications,
- Install anti-virus software,
- Register the machine to the network and user,
- Establish restrictions on what the user can do to change or install applications,
- Provision the machine in your network firewall,
- Configure the computer's software firewall,
- Set up a virtual private network (VPN) connection,
- Incorporate the computer into your data loss prevention system,
- Install and configure device management software,
- Verify that the employee has attended the security policies and procedures class, and
- Meet in person to provision and integrate their biometric access device and computer.

Environmental controls can make penetrating the perimeter or masquerading as an insider more difficult, but by no means impossible. They do little to keep technically-skilled malicious insiders from exfiltrating data, or prevent data loss from lax or socially-engineered insiders. If we have learned anything in the last three decades it is that, despite our best efforts, the perimeter can and will be breached, it is foolish to assume that all trusted insiders are in fact trustworthy, and employees don't always follow the cybersecurity rules.

Data-centric controls operate both within and across environments. The default state of the digital data that the Framework is supposed to help protect is *uncontrolled*, that is, it is freely usable. For example, an exfiltrated Microsoft Word file containing confidential information can be read by anyone with Microsoft Word software or any number of free downloadable readers. Data-centric controls change the default state of digital data to *controlled*.

Controlled data is unusable until the conditions set by the data's owner are met. If a Microsoft WORD document containing confidential information is exfiltrated, data-centric controls make certain that only authenticated users can open the file, and furthermore the owner can inhibit printing, forwarding, copy and paste, and export of the file to an

unsecure state.

Data-centric controls integrated with existing environmental controls are required to actually achieve the Framework's goal of preventing data loss. Use of both enables applications to evaluate their computing environment and determine if digital data should be made usable. For example, data-centric and environmental controls working together can assure than only an authenticated user, using an authenticated device, using an authenticated application can open a given file and enable the application to report when, where, and by whom files were accessed. Only when data owners can predetermine if, how, when, where, and by whom their data can be used, regardless of who's computer it's on, can they achieve the degree of control necessary to eliminate or greatly reduce data loss—which is the goal of the Framework.

Accounting for the Non-Linear Threat

Granted, many potential Framework implementers are missing basic controls and will benefit from implementing controls cited in the Framework. Even basic controls can be effective at stopping many nuisance and relatively unsophisticated attacks. However, basic defensive controls do little to deter sophisticated attackers.

Cyberattacks and attackers are non-linear; they range from script kiddies out for a cyber thrill ride up to highly sophisticated nation states and organized criminal enterprises. The sophisticated ones will not be much deterred by conventional defenses. They will blitzkrieg, that is, focus their attention and resources on fast, concentrated attacks designed to breach the perimeter of their highest value targets. While we are busy building cyber Maginot Lines, they will be figuring out how to breach or circumvent them. They will not wait for a standards body to ponder and eventually promulgate a standard; they will develop and deploy new attack technologies are rapidly as they can.

Implementing the Framework as it is currently envisioned will succeed in lessening nuisance attacks but will fail to secure high-value critical infrastructure targets. That is not the objective of Executive Order 13636.

NIST is Accountable for Clarity

NIST just lead a national exercise to sort out what is needed to protect our critical infrastructure. NIST knows what some of the technological gaps are. The data centric controls gap is one. Other gaps came up frequently during the Framework workshops we attended. One was (1) effective DDOS defense. Another was technology to authenticate currently installed industrial controls. There are many others that were made clear to NIST in the workshops we attended.

Industry has responded to the call and provided NIST with a clear understanding of gaps not covered by current standards. If NIST fails to make those gaps explicit to risk managers, implementers and regulators, then the Framework. is merely a repackaging of what was already known—and it's already known that the already known is insufficient.

NIST should clearly state that implementation of the Framework as it exists today is an improvement, but only a partial solution, otherwise the Framework will ultimately be seen as having made the problem worse, not better.