From: **Andrew Ginter**
Date: Tue, Apr 11, 2017 at 12:08 AM
Subject: Re: Feedback comments for NIST Cybersecurity Draft Framework version 1.1
To: "Witte, Gregory (Assoc)", Courtney Schneider, cyberframework

Hello Gregory - please find Waterfall's comments on the draft NIST framework attached.

Thank you for the opportunity to comment.

Andrew

[Attachment Below]

Comments on the NIST Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1

April, 2017
Andrew Ginter, VP Industrial Security Waterfall Security Solutions LTD.

Thank you for the good work NIST has done with the Framework for Improving Critical Infrastructure Cybersecurity, and for the opportunity to comment on the 1.1 draft of the framework. Waterfall's comments follow.

Summary

The NIST Framework for Improving Critical Infrastructure Cybersecurity, both version 1.0 and the current 1.1 draft, fail to distinguish between two very different kinds of critical infrastructures: those that focus on managing information, such as financial and e-commerce infrastructures, and those that focus on managing physical equipment, such as the electric system and petrochemical pipelines. The framework very much meets the needs of the former, information-centric critical infrastructures, where the framework's five Core Functions have more or less equal weight, and where protecting the confidentiality, integrity and availability of information are the top cybersecurity priorities for the organization.

The framework is confusing when applied to cybersecurity for critical physical infrastructures. In critical physical infrastructures, the Core Functions of Identify and Protect are much more important than Detect, Respond and Recover. The priorities for physical infrastructures are safe, reliable and efficient physical operations, not confidentiality, availability, integrity, or any other "protection of information." In addition, an important step towards clarifying guidance for physical infrastructures is terminology: the Framework should define "monitoring information" as any information leaving control system networks, and "control signals," as any information entering critical control-system networks from less-trustworthy networks. The latter must generally be inspected and secured to a much greater degree than the former.

Some practitioners already apply these distinctions correctly in their critical physical infrastructure security programs, while others do not. To be applied reliably to critical physical infrastructures, Waterfall strongly urges NIST to modify the Framework to address the essential differences between physical and informational infrastructures.

Physical Analogy

Consider a physical analogy to illustrate the point that physical and informational infrastructures must apply the NIST Framework very differently. Imagine that we are standing in the control room of a large electric power plant. A stranger walks into the room without identification, and without any sort of escort. The stranger pushes the power plant operator out of her chair, picks up the mouse and starts issuing instructions to the plant's turbines, transformers and protective relays through the operator's Human Machine Interface (HMI) software system.

How long are we prepared to permit this intruder to (mis)operate physical equipment in the power plant?

If we ask this question of any person in the room, the unanimous answer will be that this entirely the wrong question. Yes, intrusion detection, response and recovery take time, but the essential question is not whether we should permit the intruder to operate our physical equipment for 24 days, 24 hours or 24 minutes. That an intruder entered the grounds and pushed the operator out of her chair represents a fundamental failure of our physical, preventive, protective security program. The real questions are "How did this happen?" and "What must we change so this *never* happens again?"

The consequences of cyber intrusions can be identical to the consequences of this hypothetical physical intrusion. A cyber intruder with control over our control systems can physically mis-operate our physical equipment in every bit the same way as the described physical intruder.

Identify & Protect vs Detect, Respond & Recover

All five Core Functions of the current 1.0 and draft 1.1 Framework are of comparable importance to information-focused critical infrastructures. Gigabytes of electronic mail messages and web pages enter all large IT networks daily. A measurable fraction of these messages and web pages contain attacks. Software systems are deployed routinely to filter out these attacks, but no filter is perfect - in even the best-trained organizations, a measurable fraction of attacks that survive the filtering function are activated by users.

The only safe assumption therefore, is that IT networks are constantly compromised. As a result, IT organizations must take steps to systematically search for compromised equipment, isolate that equipment, erase it, and restore it from backups. Incident response teams in large, critical, information-centric infrastructure organizations are occupied more or less constantly with these tasks. The Detect, Respond and Recover Core Functions are central to security programs for information-centric infrastructures.

This is not true of critical physical infrastructures. Damaged physical equipment and lost human lives cannot be "restored from backups." The most important physical equipment, for example high-voltage transformers or large, rotating equipment, is custom-built. Replacement of damaged, large, physical equipment can take months or years. Sound security programs for critical physical infrastructures reflect this reality by emphasizing the Identify and Protect Core Functions of the Framework. Every activation of Detect, Respond and Recover functions in physical infrastructure installations is an admission of an unacceptable failure of the Identify and Protect functions.

In a sound security program for physical infrastructures, the Detect, Respond and Recover functions address only those residual risks that remain due to imperfect, preventive security functions. Investments in these secondary Core Functions should reflect the degree of that residual risk. Unlike critical informational infrastructures, that physical infrastructure incident response teams fall out of practice and need to carry out periodic drills reflects a sound emphasis on Identify and Protect Core Functions.

Again, intrusion detection takes time. How long are we prepared to permit intruders to mis-operate our physical equipment? All of this should be described in the new version of the Framework.

Safety and Reliability vs CIA or AIC

The first priority for cybersecurity at physical industrial infrastructures is never confidentiality, availability or integrity, but the protection of the safe and reliable operation of the physical process. This is not called out consistently in the draft document. For example:

- The sentence starting on line 793 of section 4.1 on pp 22 should read "Cybersecurity's primary role is the preservation of the businesses value through the protection of the confidentiality, integrity, and availability (CIA) of the organization's information, operations, and processes in critical information infrastructures. In critical physical infrastructures, the primary rolre is the preservation of business value through the protection of safe, reliable and efficient operations of physical processes in critical physical infrastructures."

- The "Protect" Function on pp 8 should be defined as "Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure products and services."

- The example at line 832 on pp 24 could better emphasize the primacy of physical continuity at physical infrastructures if rephrased as "A Senior executive held accountable to this outcome might be measured using a lagging metric of percentage uptime of physical infrastructure, with a leading metric of creating and communicating strategy for the development and implementation of control systems cybersecurity programs and systems."

- PR.AT on pp 33 should be defined as "The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements."

• PR.AT-5 on pp 34 should be defined as “Physical and cybersecurity personnel understand roles & responsibilities.”

Many other examples exist. I recommend re-reading the document in its entirety from the perspective of a security practitioner concerned very much with safety and reliability, and very little with preventing unauthorized disclosure of information about the critical physical infrastructure.

Information vs. Control

A third essential difference between physical and informational critical infrastructures is that computers controlling physical infrastructures generally require almost no information from less-trustworthy networks to operate safely and reliably. Control systems for physical infrastructure may send large amounts of monitoring information to IT Networks and to the Internet, but generally accept little or no information from either the Internet or IT systems. Furthermore, it is vital that what little information is accepted from less-trustworthy external systems is subjected to the highest possible levels of scrutiny, to ensure that such information poses no significant threat to safe, reliable operation of the physical infrastructure.

The NIST Framework, current and draft, makes no distinction between monitoring and control information flows, and describes not at all why or how control information should be subjected to much greater scrutiny and protections than monitoring information.

To this end, I recommend a change in vocabulary. “Monitoring information” should be defined as any information flowing from control system networks to external networks. “Control signals” should be defined as any information or message that flows from external sources into critical control systems.” The discussion around these definitions should emphasize that:

• Monitoring information is typically high volumes of information, while control signals are typically very small by comparison,

• Monitoring information generally flows from highly-critical physical infrastructure to less-trusted information-centric networks, while control signals flow in the opposite direction, and

• While control signals must be subjected to the highest levels of scrutiny when entering critical networks, interfering with monitoring information generally presents no greater threat to a critical infrastructure business than does interfering with any other information flow.

An example to drive this last point home: in the most dangerous physical infrastructures, such as nuclear reactor control systems and railway switching systems, control signals from less-trustworthy networks are generally filtered through the mind of the human operator, rather than trusted to any firewall or other software filtering mechanism. Human operators carefully consider instructions they receive from external sources and only when they agree that these instructions pose no threat to continued safe or reliable operations, do the operators carefully transcribe these very small instruction sets from IT workstations into their critical HMI workstations.

Specific examples of where this distinction could be made in the draft 1.1 Framework include:

• The definition of “cybersecurity” on pp 47 of the draft should not be defined as protecting “information,” but rather as “the process of protecting information and control signals by preventing, detecting, and responding to attacks.”

• The name of the “Information Protection Processes and Procedures” Category on pp 8 should change to “Information and Control Protection Processes and Procedures.”

• ID.SC-2 on pp 30 should read “Identify, prioritize and assess suppliers and partners of critical information and control systems, components and services using a cyber supply chain risk assessment process.”

The framework should draw this distinction early in the document, and apply it consistently to discussions involving critical physical infrastructures throughout the document.

Summary of Recommendations

To summarize, we recommend that the new Framework should:

1. Call out essential differences between the two kinds of critical infrastructures – information-centric and physical-infrastructure-centric,

2. Emphasize that, for critical physical infrastructure control systems, the Identify and Protect Core Functions are almost universally much more important than Detect, Respond or Recover,

3. Emphasize that the safe, reliable and efficient operation of physical infrastructure is the overriding cybersecurity priority at most critical physical infrastructure sites, and

4. Emphasize the differences between monitoring information and control signals in physical infrastructures, and how the latter must be subjected to the highest practical levels of inspection for threats to safe and reliable physical operations.

Some owners and operators of critical physical infrastructures currently understand these distinctions and apply the distinctions to the NIST Framework and to security programs routinely and correctly. Others do not. NIST has a responsibility to educate security practitioners as to the essential cybersecurity differences between physical critical infrastructures and informational critical infrastructures.

These distinctions will become increasingly important as the NIST Framework is applied to the "Industrial Internet of Things" and other initiatives that result in ever-greater integration of critical control system components with information systems and Internet-based information systems.

Further Reading

Thank you for the good work you have done in producing the NIST Framework to date, and for the opportunity to comment on, and hopefully improve, the 1.1 draft.

My comments above are a summary of the position I take in my most recent text *SCADA Security, What's broken and how to fix it,* ISBN 978-0-9952984-0-8, especially:

- Chapter 2 – SCADA Security/Section 2.7 – Safety and Reliability,
- Chapter 4 – Failure of Defense in Depth/Section 4.4 – Hacktivists,
- Chapter 5 – Preventing Intrusion, and
- Chapter 8 – Security Programs/Section 8.1 – The NIST Framework.

I recommend the text to readers who would like to explore these topics in greater depth.

For More Information

Please contact Waterfall Security Solutions directly for additional information on this topic or on any topic related to Waterfall products.

20130 Lakeview Center Plaza, Suite 400
Ashburn, VA 20147, USA
http://www.waterfall-security.com info@waterfall-security.com