National Institute of Standards and Technology RFI
(Docket Number 130208119-3119-01)
Developing a Framework to Improve Critical Infrastructure Cybersecurity

Lauren Edwards
AirPatrol Corporation
410-794-1213
ledwards@airpatrolcorp.com

Introduction

The creation of the Cybersecurity Framework is necessary for the future of critical infrastructure security. When dealing with cyber, we must realize that it changes daily and sometimes dramatically. The most impressive change to cybersecurity has been with the infiltration and exponential growth of mobile devices. A security gap often ignored, mobile devices can be a large source of data exfiltration, espionage, malware dissemination and overall increase of risks related to organizational missions and business functions.

Summary

The introduction of mobile devices into agencies and corporations worldwide due to policies such as BYOD (Bring Your Own Device) is a headache to IT and poses a significant problem to security. The best way to protect against mobile device threats is to know your wireless environment and determine the types of permissions allowed to mobile devices according to location, such as inside your company and on your network or outside. With continuous wireless monitoring, precise indoor locationing and reporting, enterprises are empowered to define current threats, act on them, and create policies to protect against them in the future.

The 20 Critical Security Controls for Effective Cyber Defense released by SANS and CSIS (Center for Strategic and International Studies) is said to reduce “measured” security risk by 94% (http://www.sans.org/critical-security-controls/). These controls include mobile security topics such as:

1. Inventory of Authorized and Unauthorized Devices
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defenses
7. Wireless Device Control

Comment Sections:

- *Current Risk Management Practices*
  1. The greatest challenge in improving cybersecurity practices across critical infrastructure is securing without limiting employees’ functionality. For example, the influx of mobile devices into the corporate environment is a result of employees’ desire for mobility and greater flexibility but if these devices are locked down or forbidden, employees are not only unhappy but also are not as efficient as they could be. In many cases employees bypass these restrictions in favor of convenience thus unwittingly exposing the organization to enhance risk. Security

without changing the purpose of mobility is a challenge faced across all organizations.

2. The greatest challenge in developing a cross-sector standards-based Framework for critical infrastructure is dealing with mobility and cybersecurity on an individual basis instead of looking at the bigger issues and determining simple solutions that will work in a variety of situations. For example, trying to secure infrastructure for each of the many operating systems and devices used by employees and visitors is not only illogical but may be impossible. It is necessary to solve the larger issues such as what all devices should be able to do in what location and in what context – for example, no use of camera while in the board room or SCIF - and apply it to all organizations.

3. The best way to measure and control risk is to have continuous situational awareness of the wireless environment. As you cannot protect against something you are unaware of, a complete real time wireless picture of all devices connecting to networks, communicating with outside sources and physically inside your organization is important. Both wifi only and cellular devices of any operating system are capable of unknowingly operating with dangerous malware that may hack sensitive or confidential information to outside locations without the user's permission. With precise locationing, rogue access points and unknown devices can be easily found and managed or terminated.

4. Cybersecurity is no longer solely the responsibility of the IT department. As the physical and cyber worlds collide, executives and IT support need to both be involved in decisions regarding how to properly secure their enterprise. The element of location and context is becoming more important as many employees work remotely and often from unsecure network locations such as a local coffee shop. Executives must cooperate with IT to create and enforce mobile device policies that apply to a variety of locations and protect the infrastructure's cybersecurity.

5. Cybersecurity risk can be defined as any event that endangers a corporation's assets via non-physical means such as wireless, networks, digital capture, etc.

6. Cybersecurity risk should now be an integral part of organizations' overarching enterprise risk management. Although some ignore the risk and hope that "it won't happen to me," a number of large, public companies with extensive cybersecurity measures in practice have been hacked with confidential information leaked (CanTech, 2013 http://www.cantechletter.com/2013/02/nortel-syndrome-why-large-companies-will-continue-to-be-hacked0221/). Small companies are also a target as they are seen to have intellectual property (IP) that is innovative and worth a large sum to the right buyer (CNBC, 2013 http://www.cnbc.com/id/100532366).

7. Reporting solutions that monitor and detect wireless and cellular activity in an enterprise with contexts such as precise location and user role are good tools to understand risk. Once risk is known, current mobile device policies and management guidelines can be altered to better control present and future risk. Mobility and cybersecurity are constantly changing and the procedures to control related risks must grow with them.

8. Required reporting of cybersecurity events has been a hot topic recently as privacy issues have been addressed with the highly debated Executive Order on Cybersecurity (http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-

infrastructure-cybersecurity) and CISPA (Cyber Intelligence Sharing and Protection Act). However, with that said, many companies are coming out with breach reports voluntarily (WashingtonPost, 2013 http://articles.washingtonpost.com/2013-03-01/world/37371617_1_private-sector-network-security-fifth-third-bank). In the healthcare sector, HIPAA (Health Insurance Portability and Accountability Act) and HTECH (Health Information Technology for Economic and Clinical Health) are enforcing regulations to increase cybersecurity.

9. No comment.

10. Performance goals for evaluating the success of mobile device policies such as BYOD and working from home can include listening to employees regarding how their efficiency and morale has been impacted by the flexibility. Good policies are created through listening to feedback and ensuring that security is not affecting usability. Policies that incorporate location through the creation of zones where different policies are active, ensure security and access to necessary device functions.

11. No comment.

12. National and international standards should create a best practices document on how to secure cybersecurity infrastructure. Overarching ideas such as continuous monitoring, user roles, location, contextual awareness and real time mobile devices management should be built into standards. As individual organizations adopt these broad policies, they can be tailored to meet specific characteristics of the organization. However, ideas such as dynamic, context-driven policy changes on mobile devices to ensure security of the user, device and data must be included at all levels of policy. With conformity on overarching policies, cooperation between organizations will be simplified as security practices will be in-sync.

- *Use of Frameworks, Standards, Guidelines, and Best Practices*

  Please see above and below comments and recommendations.

- *Specific Industry Practices*

1. Critical infrastructure organizations are interested in monitoring and detecting all wireless and mobile devices in an area. Not only does this help enforce "no wireless" areas, but it can significantly decrease the risk of data leakage through mobile devices. Through continuous monitoring, it is possible to do historical reporting of usage spikes. Also, with proper forensic enabled mobile device monitoring and management, it is possible to track where individual users or employees are via their mobile device which acts as an authorization of users accessing systems and confidential areas.

2. Practices around mobile security such as monitoring are easily integrated into existing international standards. Since mobile security exists in the convergence of cyber and physical security, location-based context-aware mobility is complementary to existing security practices.

3. The most critical ideas for the secure operation of critical infrastructure are continuous monitoring of all wireless devices, identification and authorization of users accessing systems, and asset identification and management. In many secure zones, no mobile devices are allowed but are often forgotten as they've become part of our person and walk in with us. However,

these mobile devices can be used to exfiltrate confidential information via cameras, microphones, apps and more. To ensure that an area is not sending any data outside of the current organizational walls, complete wireless monitoring must be used. For example, some office equipment transmits without users knowing such as a paper shredder that tells its father company when it is ready to be emptied.

4. Mobile device security practices such as monitoring, management, incident detection tools and capabilities are applicable for all.

5. No comment.

6. Published standards currently used by organizations in the implementation of security processes may not include enough information on how to secure mobile devices. Since published standards may take years of process before the public release, the extensive capabilities of mobile devices today are not accounted for. Continuous wireless monitoring and location-based, context-aware capabilities are necessary for organizational cybersecurity.

7. No comment.

8. No comment.

9. With wireless monitoring, issues of privacy have been raised. However, there are many ways to track mobile and wireless activity without personally identifying it to an individual. Also, with mobile device management and mobile application management solutions, an individual must opt-in before their device is tracked and controlled. There are many similarities between security cameras that are currently monitoring 24/7 and sensors that are able to monitor cellular and wifi devices.

10. No comment.

11. No comment.

12. Yes, other practices should be included in the framework. These include:
    - Continuous wireless monitoring and detection.
    - Indoor locationing
    - Indoor geo-fencing.
    - Monitoring and managing wireless devices.
    - Location-based, context aware policies and controls.