CYBERSPACE SECURITY CONTINUUM

A People, Processes, and Technology Approach to Meeting Cyber Security Challenges in the 21st Century

The Cyberspace Security Continuum: A People, Processes, and Technology Approach to Meeting Cyber Security Challenges in the 21st Century

"It's long been said that the revolutions in communications and information technology have given birth to a virtual world. But make no mistake: This world -- cyberspace -- is a world that we depend on every single day. It's our hardware and our software, our desktops and laptops and cell phones and Blackberries that have become woven into every aspect of our lives…So cyberspace is real. And so are the risks that come with it…In short America's economic prosperity in the 21st century will depend on cybersecurity."[1]

-The President of the United States, Mr. Barack Obama, 29 May 2009

- January 2003 - The safety monitoring system of Ohio's Davis-Besse nuclear power plant was offline for five hours due to the Slammer Worm putting at risk the safety of both workers and local residents.
- March 2009 – In less than 30 minutes, unidentified thieves used stolen credit card information to steal millions of dollars from 130 ATM machines in 49 cities around the world. Given the prevalence within the global marketplace for e-banking and mobile banking applications, data integrity and security of financial information is critical for continued growth.
- July 2009 - South Korea was hit by a wave of cyber-attacks aimed at paralyzing the country's largest banks, major news agencies, and government systems including the Korean Ministry of Defense. Similar threat vectors could be used against public and private sector activities in the United States.
- July 2010 – The computer worm Stuxnet is discovered. The worm initially spreads indiscriminately but is designed to target computer systems that are configured to control and monitor specific industrial processes potentially affecting critical infrastructure in the United States.
- August 2012 – A sophisticated virus called Shamoon infected computers in the Saudi Arabian State Oil Company Aramco. Shamoon included a routine called a 'wiper', coded to self-execute and this routine replaced crucial systems files and also inputted additional garbage data that overwrote all the real data on the machine. More than 30,000 computers that it infected were rendered useless and had to be replaced.
- October 2012 – Large U.S. financial institutions are hit by Distributed Denial of Service attacks. These attacks delayed or disrupted services on customer websites potentially resulting in loss of confidence for public and private institutions.

Information Technology (IT) has become more prevalent throughout the Emergency Services sector and with this increased reliance comes increased responsibility and accountability toward identity, access, and data security management. Unfortunately, the amount of information and guidance available to assist in making cyber security decisions can be daunting while the breadth and depth of the cyber security challenge can overwhelm even the most "IT savvy" manager. The Interagency Board (IAB) for Equipment Standards and Interoperability understands this

[1] The White House, Office of the Press Secretary; "Remarks By the President On Securing our Nation's Cyber Infrastructure"; 29 May 2009

concern and, in concert with practitioners in the field, developed the Cyber Security Continuum as a supporting tool to assist leaders and managers in both assessing their current cyber readiness posture and assisting in making critical cyber security decisions.

CYBER SECURITY GOVERNANCE

Generally, IT governance has been a subset of overall corporate governance focusing primarily on IT performance, risk management, compliance, and capital budgeting and, in many cases, organizational leadership tends to view cyber security governance as an IT function.

However, given the unique nature of the cyberspace realm, cyber security governance should be viewed as an element of corporate governance relative to IT and, consequently, address the dependency on cyberspace for organizational and operational activities.

Similar to IT governance where decision rights plays a key management role, cyber security governance maintains this role but also focuses on strategic integration, risk mitigation, and access/identity management.

PROCESSES & PROCEDURES

Processes and procedures are the cornerstone of cyber security governance and information assurance activities. Formal development, documentation, and dissemination enable the user community to rapidly identify threats and associated mitigating actions.

Established Standard Operating Procedures coupled with managed processes provide the integrating framework for cyber security defense in depth activities with operational requirements to meet mission areas.

TECHNOLOGY

Tightly coupled with processes and procedures is the technology necessary to enable defensive cyber security activities across the organization and the enterprise. In essence, technology becomes the “eyes and ears” for the cyber security practitioner while data collection, analysis, and forensics become the operating environment.

Traditionally, cyber and information security employed a siege mentality wherein defense was based on locking down the network via firewalls for blocking, intrusion detection for monitoring, and anti-virus as a means to prevent infections. However, the cyber threat is constantly evolving and this paradigm is no longer sufficient to meet the threat vectors.

The new paradigm involves both traditional and non-traditional actors that are more concerned

with remaining in the network once penetrated versus immediately exploiting the vulnerability. Consequently, cyber security activities must now include traditional cyber security activities along with data analytics, forensics, and remediation to overcome the threats.

TRAINING & EDUCATION

Many in the field tend to view training and education as nearly identical functions. The IAB membership would prefer to draw the distinction wherein training is the "Know How" and education is the "Know Why".

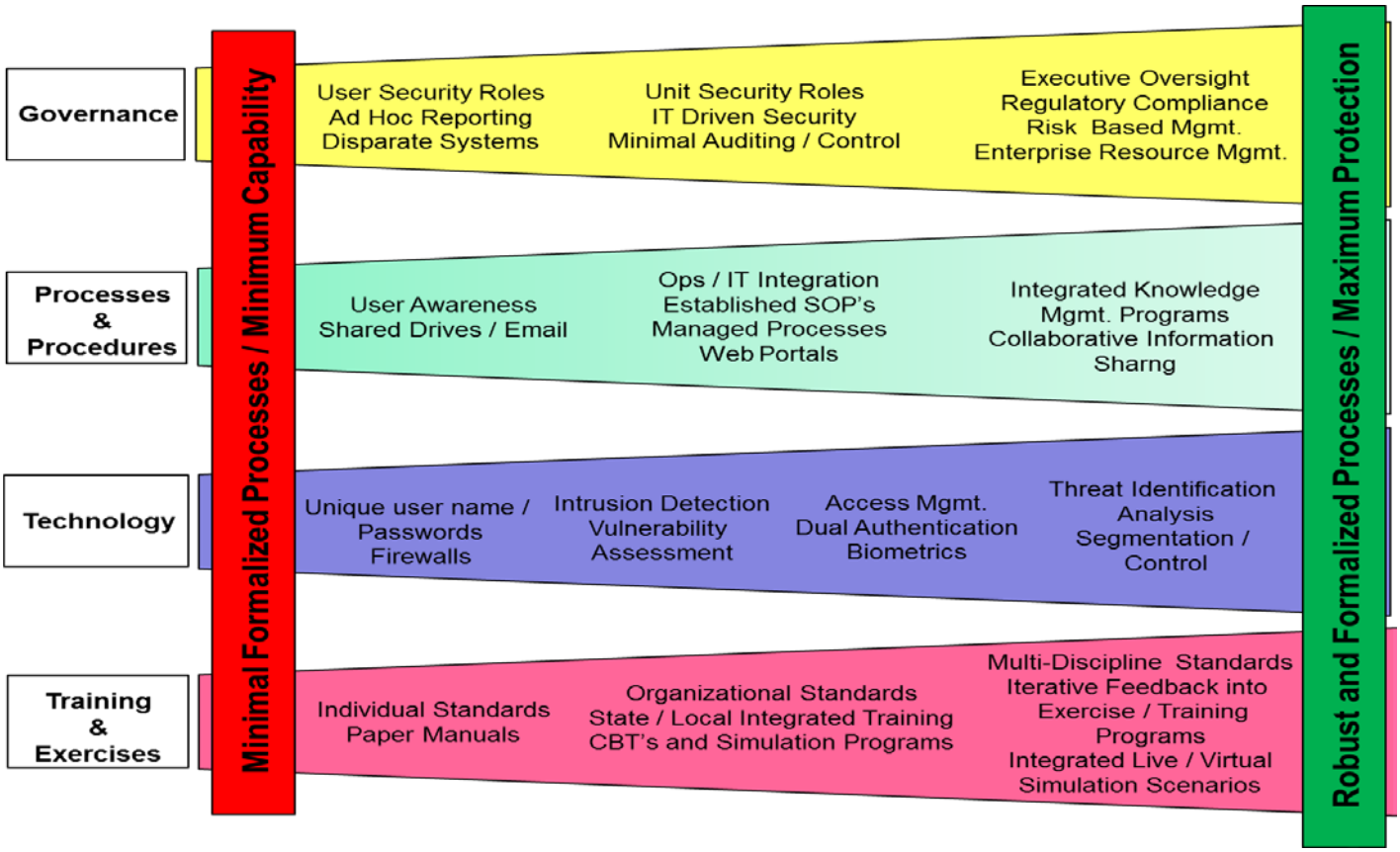
Consequently, training should focus on practitioner level activities that provide a level of competence on a variety of subjects that either directly or indirectly affect individual or unit performance. Examples of training include ad hoc sessions at the tactical level, more formalized sessions in either a classroom or computer based format, and certifications relative to position requirements.

Contrasting these activities are ones which are educational in nature and focus not on task specifications but on the macro fabric underlying the training. Examples can include certifications across multiple disciplines, formal classroom training, and accredited programs.

Attached below is the Cyber Security Continuum developed by the IAB to aid leaders and managers in assessing their current cyber readiness posture and assisting in making critical cyber security decisions. In an effort to maintain alignment with existing interoperability efforts, this graphic was adapted from the existing SAFECOM Interoperability Continuum.

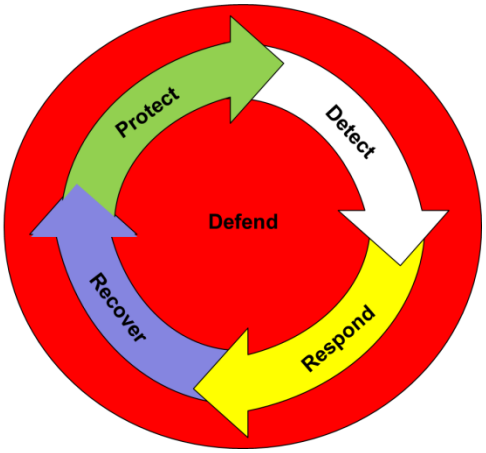
The Cyberspace Security Continuum: A People, Processes, and Technology Approach to Meeting Cyber Security Challenges in the 21st Century

Figure 1 – Cyber Security Continuum



APPENDIX A – CYBER SECURITY QUICK REFERENCE GUIDE

We live in a globally interconnected world that is both threatening and dynamically evolving. As a result, organizations, businesses, and agencies across both the public and private sector must develop and implement innovative processes and procedures to meet emerging threats while planning for future challenges. Violent extremists, nefarious state and non-state actors, coupled with transnational criminal organizations and insecurity in the global commons reflect our strategic environment for the foreseeable future.



Consequently, when discussing cyber security, an iterative approach must be used. Although there are many models, the IAB recommends the following minimum guideline:

- **Protect**
- **Detect**
- **Respond**
- **Recover**

1) **Protect:** Protection is focused on internal and external processes and procedures to create "defense in depth" approach to cyber security. Sub-elements of protection include:
    a. Unique User ID / Password
    b. Digital Token
    c. Biometrics
    d. Compliance
    e. Education / Training

2) **Detect:** Detection is the means by which organizations, businesses, and agencies identify malicious activity (either internal or external). Sub-elements include:
    a. Cyberspace Operations
    b. Network Monitoring
    c. Logging and Correlation
    d. System Security Management

3) **Respond:** Response activities are designed to counter the current threat vector through the use of people, processes, and technology. Sub-elements include:
    a. Incident Response
    b. Cyber Investigation
    c. Cyber Forensics

d. Systems Security Analysis
e. Collaboration

4) **Recover:** Recovery operations are focused on restoring core functional processes and systems to a full operating nature. Sub-elements include:
   a. Knowledge Management
   b. Data Administration
   c. Vulnerability Assessment
   d. Exploitation Analysis
   e. Test / Evaluation

As noted above, a layered approach to cyber security is necessary for organizations, businesses, and agencies to protect and restore critical information technology (IT) systems and services. Consequently, the IT professional must take proactive steps to ensure the effective, efficient and integrated operations of all organizational IT systems. These steps may include the following:

- Implement and sustain an effective and consolidated IT infrastructure
- Ensure cyber security operations are synchronized with core operational activities
- IT systems assets maintain data integrity, are resilient and secondary/tertiary systems are available to ensure effective decision making during crisis operations
- Maintain situational awareness of network intrusions or degradation to analyze threat vectors and develop recommended courses of action for the decision makers
- Implement comprehensive cyber security training objectives and assess throughout the organizational exercise cycles

Not only are the activities and processes noted above critical to maintaining cyber security but the IT professional must not overlook basic user cyber security measures. The most sophisticated cyber security architecture in the world cannot compensate for user deficiencies; therefore, proactive user education methods are recommended. Although not all-encompassing, the IAB recommends the following methods:

- Maintain separate user accounts/passwords when operating critical or sensitive IT systems
- Encourage employees to refrain from accessing unknown or potentially harmful websites – phishing actors seek to duplicate known websites therefore due diligence is required
- Encourage employees not to open emails from unknown sources
- Encourage employees not to click on embedded links without first checking the URL resolution
- Do not provide information to outside sources on organizational cyber security policies and practices

The Cyberspace Security Continuum: A People, Processes, and Technology Approach to Meeting Cyber Security Challenges in the 21st Century

- Encourage employees not to write down and/or store passwords in unsecure locations.

As today's cyber environment is fast-paced and constantly changing, the IAB understands the IT professional needs handy reference guides that are easy to understand, not only for the "cyber savvy" but for the average IT professional as well. Table 1 is a simple to use Cyberspace Security Matrix that can aid the IT professional in cyber security planning and implementation processes.

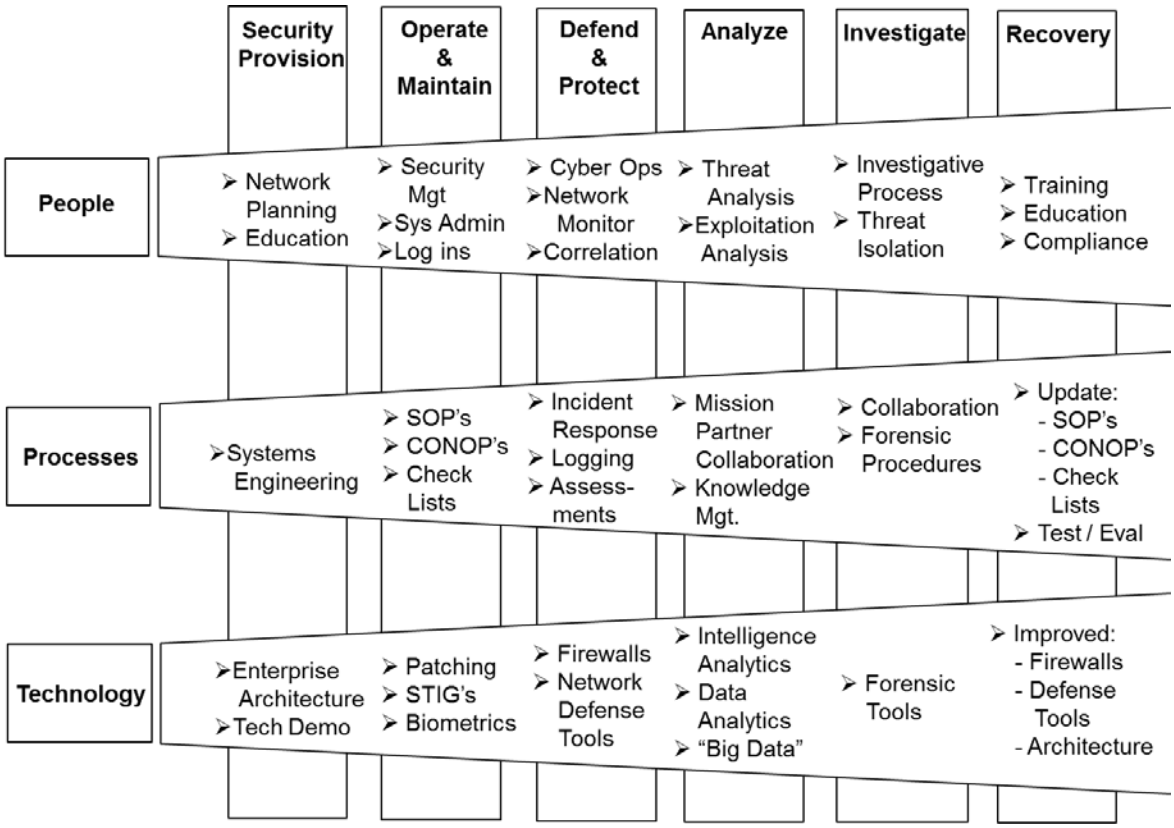


Table 1 – Cyber Security Matrix

**Please contact the InterAgency at info@interagencyboard.us with any comments, feedback, and questions. Additional information on the InterAgency Board is available at www.IAB.gov.