Risk Considerations in a Network and Security Operations Center
Maximizing Your Benefit

Edwin B. Covert

- Director of Information Security Services for Integrated Communication Solutions (ICS)
- Eleven years of experience in INFOSEC/IA with government and commercial entities
- CISSP/GCIH

Agenda

- What is an NSOC?
- Introduction
- The Process
- Assessing the NSOC
- Planning the NSOC
- Engineering the NSOC
- Managing the NSOC
- Summary

What is an NSOC?

- A NSOC is the facility and capability that allows an organization to manage critical assets in a continuous near-real-time manner
- Assets are network elements, security devices, information, etc.

Introduction

- The threat is evolving
  - Little control over it
- Mitigation strategies must evolve as well
- One of the most cost-responsible outgrowths of this strategy is the development and implementation of a Network and Security Operations Center (NSOC)

Introduction

- Several key considerations for any NSOC:
  - Infrastructure
  - Procedures
  - Personnel
- Using ICS' Information Assurance Life Cycle (IALC), let's examine these issues

What is the IALC?

- Information Assurance Life Cycle
- The IALC *makes security possible*
- Contains four components:
  - Assess
  - Plan
  - Engineer
  - Manage

Assess (Step 1)

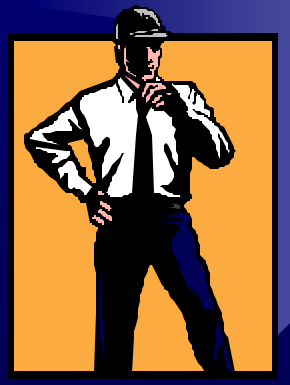
- Evaluate and audit the infrastructure and technology to determine a baseline
  - Judged against the business objectives and requirements of the organization
  - Used to provide recommendations to maximizing the value of the project

Plan (Step 2)

- Develop a plan of action to implement any new processes/technologies that will satisfy the security requirements while enhancing productivity
  - Information is derived from the Assessment phase (step 1)

Engineer (Step 3)

- Implement the solution(s) that ensure the attainment of business goals utilizing the technology and security recommendations planned
  - Information is derived from the Planning phase (step 2)



Manage (Step 4)

- Provide for the management of the solution.
  - Often the most critical step
    - Usually, the one that is forgotten
  - This ensures the continuity and accuracy of information
  - Allows for security to be maintained and updated over the long-term

The Journey

- Let's begin…

Assessing the Infrastructure

- Where should it be located
  - In a public location?
  - Remote location?
- Equipment requirements in the NSOC will dictate other factors:
  - heating-ventilation-air conditioning (HVAC)
  - physical security
  - communication necessities (network security cannot be maintained if one cannot “see” the devices that require security)

Assessing the Infrastructure

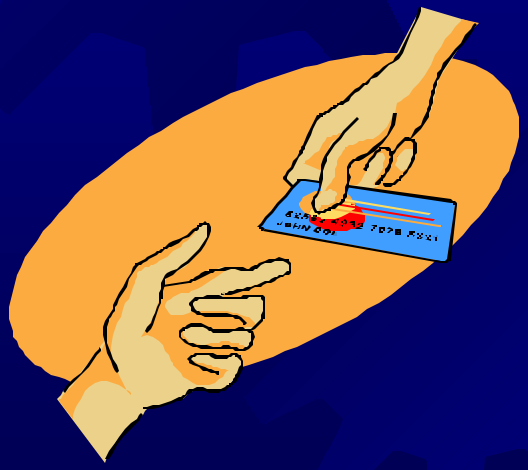
- Be aware of local, state/provincial/ territorial, and national laws on the types of infrastructure they can utilize

Assessing the Procedures

- Some laws require reporting information crimes by Internet service providers (ISP)
- How is the organization required to interface with
  - Law enforcement agencies
  - Intelligence agencies
  - Commercial and non-profit information security organizations

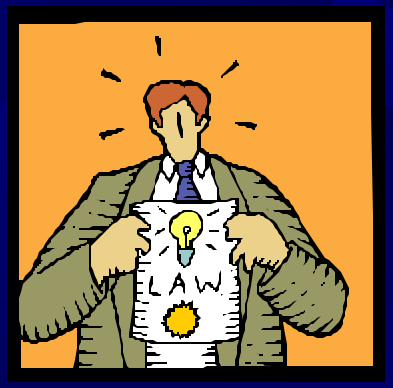
Assessing the Procedures

- Information Sharing and Analysis Center
- Organizations must consider internal reporting structures



Assessing the Personnel

- Currently, the information security services market is not regulated
- That could change drastically



Assessing the Personnel

- PREDICTION: "Certified" NSOCs will have certified incident handlers and intrusion analysts on staff for each shift
- What if the organization is going to offer its NSOC capabilities for sale to other organizations.

Planning the Infrastructure

- If building a NSOC, hire a professional management firm
- Communications Infrastructure
  - Utilize the skills of the senior-level network and infrastructure engineer

Planning the Infrastructure

- Issues
  - Timeframes
  - Circuit Convergence
  - Redundancy
  - Telephones
  - Cabling

Planning the Procedures

- Standard Operating Procedures (SOP) are an indispensable component of an NSOC
  - They ensure consistency and improve efficiency
  - Reduces “ramp-up” time for new hires

Planning the Procedures

- Form a committee (or subcommittee) tasked with developing SOPs from best-practices

Planning the Personnel

- In-house training
  - Often overlooked aspect of a training program
  - By sending a single individual to a formal training session and then having that person conduct in-house training on the subject matter can save time and money over the long term
  - Sometimes requires “Training the Trainer”

5 Minute Stretch Break

Engineering the Infrastructure

- There are too many intricacies with building a facility to go into here
- Have qualified personnel do the actual engineering
- Make sure everyone is on-board before construction begins or cable installed

Engineering the Infrastructure

- Communications redundancy = continuity of operations
  - either from a natural disaster or “back-hoe fade.”
- If the phone system is not properly installed, clients will not be able to reach the NSOC
- Electrical infrastructure components not properly installed can lead to loss of life for the organization’s employees

Engineering the Procedures

- Subject your procedures to outside review
  - This is sometimes hard
  - Hire a consulting or auditing firm to review them
- Outside review ensures essential steps are not missing from the process

Engineering the Personnel

- Hiring personnel that meet the requirements developed during the assessment phase should be the focus

Engineering the Personnel

- Experienced individuals should be able to work on any engineering issues ad hoc
- After a smooth opening operation has occurred (six to eight weeks), begin to implement the training program

Managing the NSOC

- Across the three areas (infrastructure, procedures, and personnel), managing the NSOC breaks down into two areas:
  - Tactical management
  - Strategic management

How to Manage the NSOC?

- Tactical Management
  - Concerns the daily operations that keep the NSOC a viable and effective enterprise
- Strategic Management
  - Issues that deal with how the NSOC will evolve during its existence

Tactical Management Issues

- Moving equipment (physical),
- Configuration of firewalls and other perimeter devices (infrastructure),
- Revising SOPs and policy documents (procedure),
- Ensuring the NSOC staff is effectively performing its job (personnel).
  - Watch for signs of staff fatigue or burn-out

Lessons Learned

- Location
- Circuits
- SOPs
- Personnel

Summary

- Having a NSOC is critical to successfully managing organizational assets
- Creating a NSOC is no small task
- It requires a proven methodology
  - Such as the IALC

Questions and Feedback

- Edwin Covert
  - ecovert@icscorp.com
  - 301-695-8800, 210
  - www.icscorp.com