Protecting Information In The Digital Age

Florida State Association of Supervisor of Elections (FSASE) Summer Conference

June 21, 2017

Presented by: Billy R. Hall, President and CEO, NetIT4u, Inc

Security is Everyone's Responsibility — See Something, Say Something!
A List Of Things That Are Invisible

1) 
2) 
3) 
4) 
5)
The following presentation was based off of an Air force briefing. Though the concept is primarily used throughout the military, it can be applied to all government agencies.
Objective

- Understand the core of Protecting Information or Operation Security (OPSEC)
- Define & identify targets and threats
- Establish countermeasures
- Identify the Critical Information Commandments
- Decipher the value of information
What is OPSEC...?

- Have you ever taken precautions against someone...
  - ...breaking into your house while you’re on vacation?
  - ...stealing your purse?
  - ...stealing packages from your car while you’re shopping?
  - ...fraudulently using your credit card?

Then you have used OPSEC!
What is OPSEC...?

- OPSEC is a risk management instrument that enables a manager to view an operation or activity from the perspective of an adversary. It is a process of identifying, analyzing and controlling critical information.
What is OPSEC...

- Identify Critical Information
- Analyze Threats
- Discover Vulnerabilities
- Assess Risks
- Develop Countermeasures

Security is Everyone's Responsibility — See Something, Say Something!
What is OPSEC...?

- Identify Critical Information:
  - Credit card numbers, travel dates, itineraries, passwords, patterns, changes in patterns, inspection results, information base systems, etc..

- Analyze Threat:
  - Adversaries, Intelligence agencies - Open source information, corporate/state sponsored spies, eavesdropping, photographing, etc...
What is OPSEC...?

- Discover Vulnerabilities:
  - Flow of information, operations, timing of events, how an adversary would acquire the information, etc...
    - How would the loss of such data impact the organization?

- Assess Risks:
  - Estimated loss $ \times $ impact of risk $ \times $ likelihood of risk $ = $
    Does the solution outweigh the loss?

Security is Everyone's Responsibility — See Something, Say Something!
What is OPSEC...?

• Develop Countermeasures:
  - are based on the vulnerabilities and inherent risks.

• Are dictated by cost, timing, feasibility, and imagination of involved personnel. Simplicity, straightforwardness, and inexpensiveness are key to the most effective countermeasure solutions.

OPSEC is a DIFFERENT WAY of SEEING
How Do I Identify Threats & Vulnerabilities...?

- Take note of suspicious behavior
  - Be aware of your surroundings, know your environment, and personnel
    
    If you see something, say something

consistent with the testing of systems

- There is always room for improvement
Critical Information Commandments...

1. Thou must protect the information that the adversary needs to accomplish his mission.
2. Thou shall not try to protect everything.
3. Consider who thy adversaries are and what information they require to inflict harm to you.
4. Thou shall consult all sources of information to determine what thine enemies know about you.

5. Once thou has determined what information is critical, thou shall determine if that information is associated with thine activities.
What Information Should I Protect...?

- Information that the adversary needs to accomplish their mission.
- Intelligence information on programs associations
- Technical information on communications
Orchestrating security technology

To tackle advanced threats in an ever more complex cyber world, agencies must integrate all their security tools, data and processes.

BY DAVE McCLURE

The plethora of security analytics tools available to federal agencies has helped improve cyber incident and vulnerability prevention, detection, response and recovery. However, significant challenges remain as types of attacks and attack vectors increase. Indeed, agencies are finding they often need to integrate or "orchestrate" existing analytical tools, processes and data into repeatable, automated workflows to fully support solid security operations.

Concurrently, architectural challenges abound as cloud services, mobile technology and Internet of Things devices rapidly generate increasing amounts of data, new system endpoints and network traffic flows. Newer cyber analytics that use machine learning are of primary interest because rule-based or signature-based prevention tools struggle to detect or stop advanced cybersecurity threats.

Here are some key observations and lessons learned to date in the cyber analytics area:

1. Security analytics require orchestration. There are a wide range of commercial products and open-source tools that agencies can use to perform analytics, but agencies should not fool themselves. The full value of enterprise security analytics cannot be gained simply by installing hardware or network appliances.

Federal agencies are building systems that ingest terabytes of security data, but their analytics can only process tens of events per minute. Even with fantastic visualization tools, analysts will only be able to manually process tens of events per hour. Tools can help perform a dataset to a meaningful analysis after the fact. The key question is whether they can be used correctly.

Security analytics tools

- Security incident and event management
- User and entity behavior analytics
- Intrusion prevention systems
- Network traffic analysis
- Endpoint protection platforms
- Endpoint detection and response
- Data loss prevention
- Data exfiltration analytics
- Identity and access management analytics

Security is Everyone's Responsibility — See Something, Say Something!
Security is Everyone's Responsibility — See Something, Say Something!
Federal Computer Week Article

Cybersecurity by the Numbers

16 | The number of cyber-incidents considered “major” by federal agency heads, out of nearly 31,000 incidents

46 | The average amount of days it takes to resolve a cyberattack

50 | The percentage of attacks that will use SSL/TLS encryption to avoid detection

300 | The percentage of increased ransomware attacks nationwide in 2016 over 2015

1,300 | The percentage of increased cyberattacks in federal agencies over the past ten years

4,868 | The number of federal cyberattacks, out of nearly 31,000, reported as web-based or web application-based attacks

21,155 | The average cost of a data breach, per day

3.1 billion | The proposed federal budget for cybersecurity and modernizing IT

Security is Everyone’s Responsibility — See Something, Say Something!
Security Checklist Considerations

Identify and Assess Critical Election Systems

- Define Your Inventory
- Regular Assessments
- Catalog/Improve
- Disasters

Security is Everyone's Responsibility — See Something, Say Something!
Security Checklist Considerations

Physical Security

• Office
• Warehouse
• Server Room/Data Center
• Authorization Policy

Security is Everyone's Responsibility — See Something, Say Something!
Security Checklist Considerations

Network Security

• Vendor/Partner Plans
• Controlled Access
• Outside Connections
• Monitoring
• Anti-Virus

Security is Everyone's Responsibility — See Something, Say Something!
Security Checklist Considerations

Acceptable Use Policy

- Written
- Enforcement
- System Enforcement

Security is Everyone's Responsibility — See Something, Say Something!
Security Checklist Considerations

Worst Case

- Critical Failure
- Physical Compromise
- Un-Authorized Access
- Public Perception

Security is Everyone's Responsibility — See Something, Say Something!
Security Checklist Considerations

Restoration

- Accessible Backups
- Offsite Location
- Vendor Support
- Staffing

Security is Everyone's Responsibility — See Something, Say Something!
To try to obtain financial or other confidential information from Internet users, typically by sending an email that looks as if it is from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one.
Security Checklist Considerations

Phishing
Security Checklist Considerations

Phishing

- Recipients
- Education
- Compromise
- Reporting
- Internet Use

Security is Everyone's Responsibility — See Something, Say Something!
Be Vigilant, Be Prepared!!

- Remember Protecting Information in the Digital Age is a forever more moving and changing environment. Don’t be frustrated, just keep moving your efforts forward - there are no absolutes or fool proof solutions - Do Something Doing Nothing is a certain failure!
Conclusion...

• OPSEC is critical to Your Security
• Make sure you have someone managing your Security Efforts
• Don’t have one appoint one

My Security Manager is ???

Security is Everyone's Responsibility — See Something, Say Something!