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

A List Of Things That Are Invisible

1)

2)

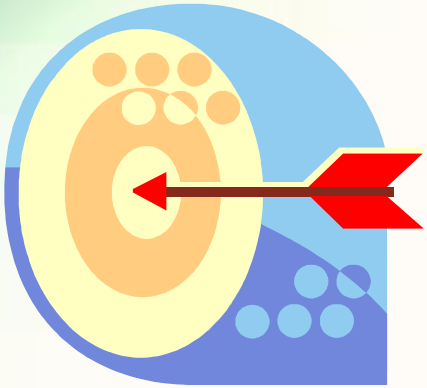
3)

4)

5)

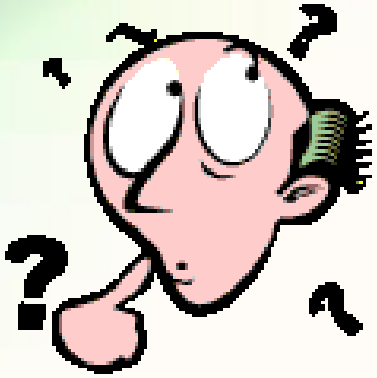
The following presentation was based off of an Air force briefing. Though the concept is primarily used throughout the military, it can be applied to all government agencies.

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 your shopping?
  - …fraudulently using your credit card?

Then you have used OPSEC!

netIT4U

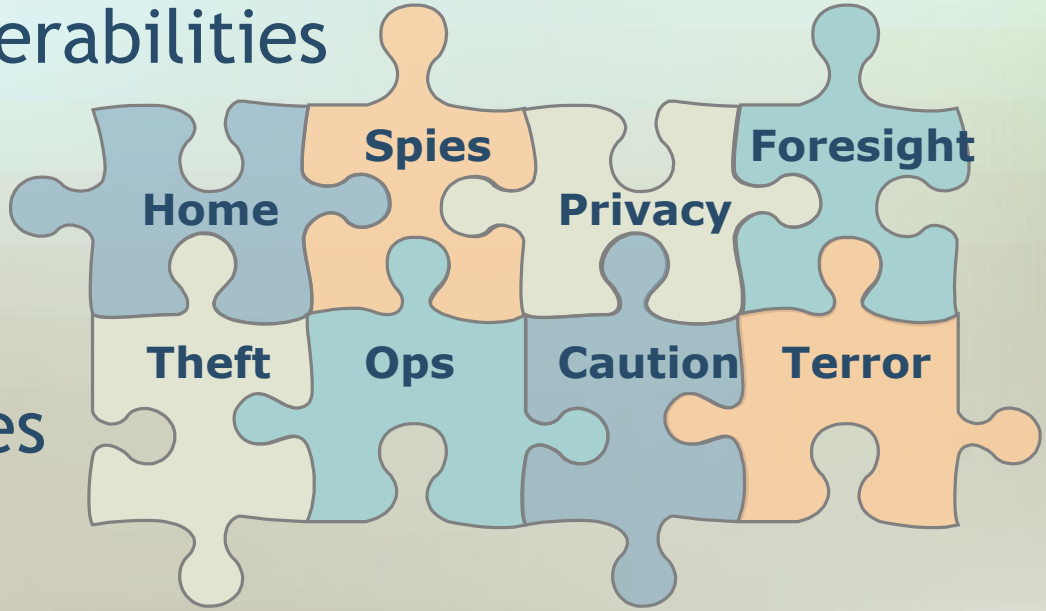
What is OPSEC…?

- 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



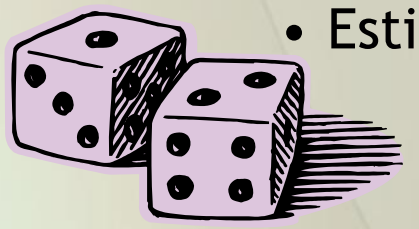
What is OPSEC…?

- 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 $ x impact of risk x likelihood of risk = $

    Does the solution outweigh the loss?



netIT4U

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

netIT4U

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.

netIT4U

Critical Information Commandments…

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

Federal Computer Week Article

DrillDown

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 cyber-security 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 analysts can only read triaged data at a few events per minute. Even with fantastic visualization tools analysts will only be able to menta process tens of events per m

Tools can help pare dataset to a sma analysts also questions use ca insi

say tool i

gencies ofte ecurity tool in indepen dent silos, and many of the invoke duplicative capabil ties from different vendors sometimes on the same sys tem. Security analytics wi need to connect those silo and automate processes an investigations across thos tools until they evolve to th point where they function a a "force multiplier" for bette threat detection.

2. Accurate inventorie of networks, systems an endpoints are essentia

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

Source: Gartner

28 May 2017 FCW.COM

Federal Computer Week Article

Shadow IT — a combination of unauthorized and unidentified solutions — is a growing problem for federal agencies. Audits by inspectors general and the Government Accountability Office demonstrate the lack of complete knowledge about what resides on and interacts with agency networks (hardware, software, mobile, IoT, etc.). Agencies cannot protect what they don't know about.

Fortunately, new tools are much better at tracing networks and detecting/identifying devices. Security analytics correctly applied to network traffic helps shine light into the shadows.

3. People trained in advanced analytical tools are crucial. Federal CIOs, CTOs and chief information security officers must hire and retain the right team for security analytics and treat it as an ongoing investment. Security analysts must be curious, explore the high-value anomaly data they collect, trace unusual patterns and follow the trail of an investigation wherever it leads.

Looking at individual or correlated events is not sufficient anymore. That approach is being augmented by a rise in "offensive hunting" in which highly trained analysts emulate bad actors (hired hacktivists, rogue nation-states, insider threats) and their tactics to penetrate networks, devices, applications and systems.

Advanced security analytics requires bridging two new professional domains: hacking and data science. Most experts specialize in one or the other but not both. Accordingly, data scientists and security experts need to work together to enable the use cases that are essential to good security diagnostics and continuous monitoring.

Agencies still need competent security analysts to tweak models, confirm "good" versus "bad" anomalies and analyze critical outputs of agentless appliances. Although red teams and hunt teams play a separate role in cyber defense in larger organizations, skills and experience are in short supply and often an outsourced capability.

There is no single tool, no single database and no single approach to solving a cyberthreat problem.

Those capabilities, combined with effective incident response processes, are critical for continuous security improvements and a full understanding of different types of attacks, including commonly used phishing and other social engineering techniques.

More important, agencies must set up cyber analytics to fit their risk profile and threat vectors. It is not uncommon for agencies to drop sophisticated tools into their networks without having skilled employees do the required tuning to optimize detection and protection for specific and unique threat ecosystems. One size does not fit all, but going with default settings is creating such an environment, which is easy to breach and attack using zero-day exploits with far-ranging impacts.

4. Continuous monitoring must include continuous data sharing. Critical data for cyber analytics is typically not owned by the security departments. Instead, the business or program side of an agency is the data owner and access controller. Well-defined cyber and data governance and stakeholder management are needed to tackle that complication. Additionally, proper processes and technology are the key to collecting and delivering the right data.

Security officials should reset current approaches by clearly defining what they want to achieve with cyber analytics, followed by consideration of three key initial steps:

- For agencies still relatively new to the cyber analytics space, it might be worthwhile to explore the open-source versions of tools or, alternatively, pursue time-bound pilots or "proofs of value" that can be up and running with demonstrated results in days or weeks before jumping to advanced tool acquisitions. That approach can help garner executive support and gain the IT team some experience with the tools.
- Agencies should follow a strategy and roadmap that embrace the idea that there is no single tool, no single database and no single approach to solving a cyberthreat problem. Locking into a vendor/solution in an evolving market could be premature, particularly if that vendor is not tuned into changing threat environments. Security analytics should complement diverse strengths rather than compete against one another.
- Setbacks should be expected. Security analytics will not solve all detection problems or pinpoint every threat. The tools can, however, reduce alert volumes and false positives, identify previously unknown threats, and uncover abusive insider threats. Agencies must learn from each journey down thorny cybersecurity pathways — from their own mistakes and those of others. Continuous adaptation, learning and adjustment are necessary in such a complex and ever-changing cyberthreat environment. ■

Dave McClure is chief strategist at Coalfire Federal.

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 Checklist Considerations

Identify and Assess Critical Election Systems

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

Security Checklist Considerations

Physical Security

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

Security Checklist Considerations

Network Security

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

Security Checklist Considerations

Acceptable Use Policy

- Written
- Enforcement
- System Enforcement

Security Checklist Considerations

Worst Case

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

Security Checklist Considerations

Restoration

- Accessible Backups
- Offsite Location
- Vendor Support
- Staffing

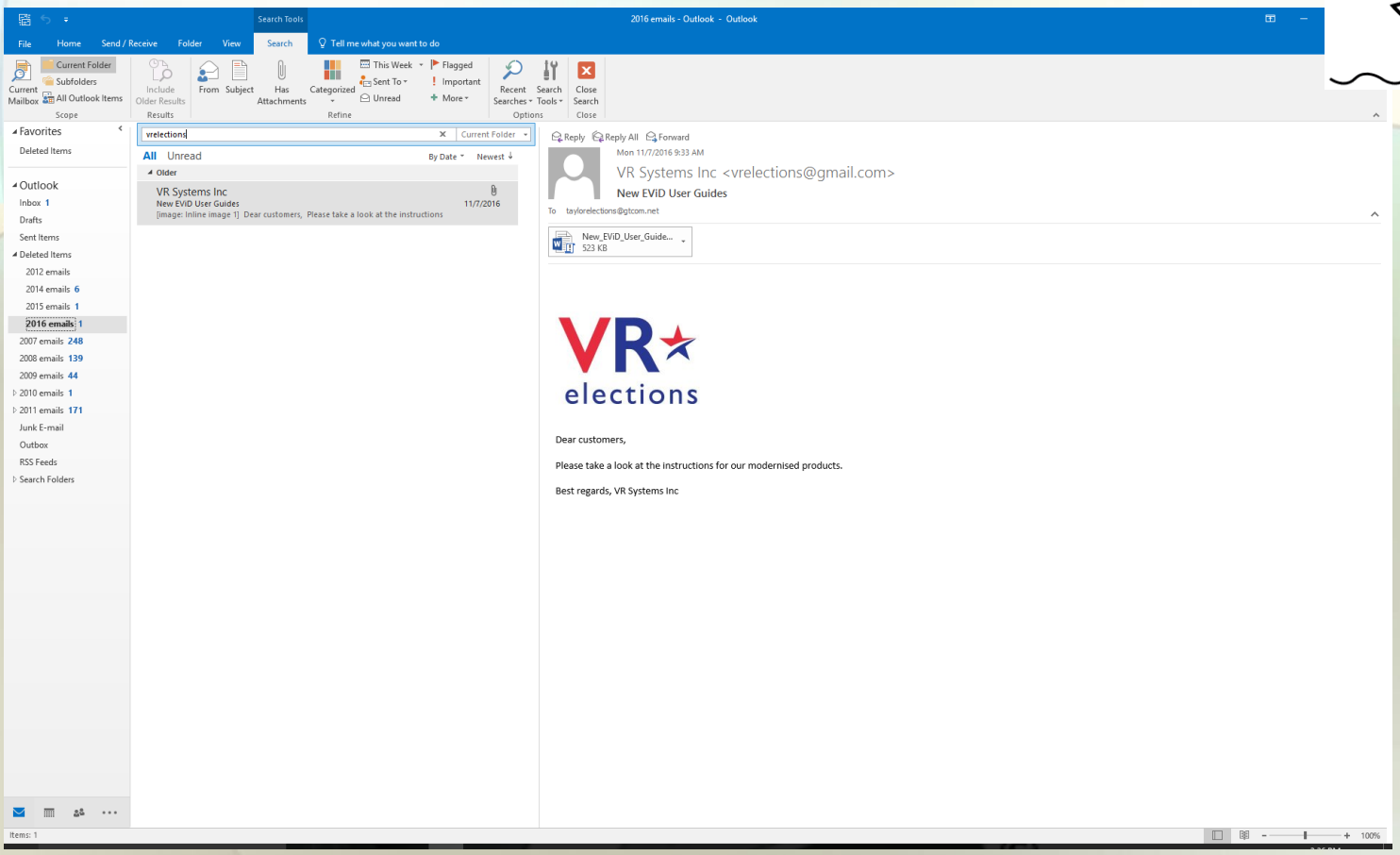
Security Checklist Considerations

Phishing

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

netIT4U

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