Re-tooling Your Cybersecurity Program: From Staffing to Operational Execution

Thursday, 17 May 2018

Steve Brown
Steps to Building a More Sustainable Program

1. Identifying the Primary Threat and Control Gaps
2. Taking Stock of Responsibilities/Capabilities vs Threat
3. Build a Roadmap that Prioritizes Gaps, Capabilities, Needs vs Today and Tomorrow’s Threats
Building the Roadmap

Gap Assessments
- Top to bottom assessment of current capabilities vs. optimum state

Service Catalog
- List of core services required of each organization
- Staffing requirements
- Maturity level

Prioritization
- Priority gaps vs. capability vs. future state capability
Gap Assessment – Measuring Against Known Standards

- Measure against the Threat, NOT peers
- Identify gaps not just in technology but processes, policies and personnel
- Avoid relying on a “check the box” type assessment
- Assess the whole control eco-system
  - Breadth of deployment, tuning, frequency of updates, use of logs, integration with other controls, etc.
Identifying the Primary Threat vs Controls
Gap Assessment – Measuring Against Threat

• Prioritizing remediation/mitigation efforts against the highest threats vs. highest potential impacts
  
  o Map the gaps against highest threat via kill-chain model
  
  o Look for opportunities to mitigate the threat elsewhere in the kill chain in order to provide a more flexible and cost-effective approach to defense-in-depth
Taking Stock

• Develop a Service Catalog

- List of core services each team must provide to achieve stated mission
- Corresponding staffing requirements for each service (actual vs. necessary)
- Identify Current Capabilities and Skills as well as Gaps (current and future)
- Maturity level of each service
Selling the Vision

- Program **must** be dynamic and able to adjust to emerging threat
- **Don’t** boil the ocean,
- **Don’t** cry wolf when its just a puppy,
- **Don’t** try to wow ‘em with technical jargon

**Do** demonstrate how today’s roadmap links to the next
**Do** call out the company’s most concerning threat as it applies to the ‘crown jewels’
**Do** detail precisely how new technologies and processes mitigate the threat

• Use the service catalog/gap assessment/threat assessment/18-month roadmap to convey a clear, concise, measurable plan
• Demonstrate how each milestone will address the threat in a prioritized, risk-based manner (including headcount)
Building the Team

One Team; One Mission; Many, Many Complimentary Assets

- Define swim lanes for teams while encouraging awareness of others' challenges and crossing lanes when needed
- Leverage expertise across the organization, but don't dilute by leveraging one asset too much
- Use tiger teams to solve difficult problems in a hurry
- Cross train and enable senior managers
Overcoming Cultural Barriers

Going Beyond Compliance

- Compliance is a necessary base-line that contributes to a secure environment
- Compliance **DOES NOT** equal Security; but if you do Security properly you should be compliant
- O&M is **NOT** evil

Consistent, Constant, and Persistent

- One message, one response
- Exceptions are just that and **NOT** the rule
- Focus on building a solid foundation and leave the enhancements for later (*Don't chase the Shiny Objects!*)
- Document, Document, Document – Everything can’t be fixed (although we try) but it must be documented and tracked
- Stick to the Roadmap and adjust only when threat warrants deviation
Capability Maturation & Improvement

- Once the foundation is in place; mature the processes and layer on enhancements to improve threat response against today’s threat as well as tomorrow’s evolving threat.
Cyber Security Operations
Build Out Foundation While Applying Next Generation Enhancements

24/7
Network Monitoring & Response Capability
Security Intelligence Fusion Center
Enterprise Security Data Warehouse “Cyber Data Puddle/Pond/Lake”
“Hunt” Capability
Establish a Security Risk Program  
Consistent, Constant, Persistent

- Identify and Remediate Cyber Risks
- Raise Risk Awareness
- Establish a Control Framework
- Perform Self-Assessments
- Validate Controls
- Identify, Document, Remediate/ Mitigate, and Track
Pragmatic Measurements, Reporting, Evaluations

Metrics for metrics sake are not valuable. Focus on the areas that you are trying to make progress in, and then share relevant data.

Taylor the measurements to the audience
- Executive leadership need one level of detail
- “Feet on the street” need a different level

Sometimes you need to stop and look at how far you’ve come rather than focus on how much farther you still need to travel

When dealing with overwhelming statistics, parse the data in order to identify most impactful targets for improvement
- Example: VpAs vs. total number of vulnerabilities in the enterprise