A Holistic Approach to Cyber Security

*Reduce the gap between your tools and your strategy.*

July 23, 2019
Today’s Presenters - A Holistic Approach to Cyber Security

Steve Roesing  
President, CEO, ASMGi  
sroesing@asmgi.com

Frank Yako  
CIO, Director of Strategic Initiatives, ASMGi  
fyako@asmgi.com
What If There Was A Way To Develop Your Cyber Program, such that …

- The business understands what, when and why you’re are implementing solutions?
- You determine what an appropriate budget is for the enterprise, versus being told how much budget you’ll get to protect the organization
- Each implemented solution achieves a return on its own, PLUS works well with current solutions and contributes to a larger eco-system (whole is greater than the sum of the parts)
A Holistic Approach to Cyber Security

Total Solution = People + Process + Technology
Total Solution = 3 Pillars

- Program
- Tech
- Operations
Way of thinking…

◆ The Point-Solution Mindset
  ◆ Fragmented
  ◆ Focus on Technology
  ◆ Reaction to “something” – like media = CEO
    listening to NPR on the drive to work! (event-driven, like Wikileaks = DLP)
  ◆ What the business “wants” at a point in time

◆ The Holistic Security Mindset
  ◆ Focus on Solutions = People + Process + Technology
  ◆ Gap-based + Risk-Based
  ◆ Align with the business
  ◆ What the business “needs” for the long-term
LEARN TO SEE THE FOREST
NOT JUST THE TREES
Way of thinking…

The key is not to prioritize what's on your schedule, but to schedule your priorities.

~ Stephen Covey

GoalGettingPodcast.com
How Do You Make Decisions?

- Holistic Approach or Point Solutions?
- Are your Roadmaps based on risk posture or budgets? (Are you value-based or cost-based?)
- Do you see the forest or the trees?
- Are you trying to prioritize everything, or scheduling only what you determine is a priority?
How Do you “Do” a Holistic Cyber Security Program – Quantify your Risk …

Quantifying Cyber Risk

◆ Bring security closer to the business
◆ Create a common language to discuss cyber risks
◆ Prioritization = Align budgets with initiatives that provide actual economic impact

<table>
<thead>
<tr>
<th>Recommendations (prioritized order)</th>
<th>Value Shift</th>
<th>Cost</th>
<th>Reduction In Expected Loss</th>
<th>Expected Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Today</td>
<td></td>
<td>$0</td>
<td>$9.7M</td>
<td>$21.5M</td>
</tr>
<tr>
<td>Rollout #2: Fully implement CIS Control 1: Inventory and Control of Hardware Assets</td>
<td>(77.0)</td>
<td>3,262.3</td>
<td>$6.4M</td>
<td>$157.4M</td>
</tr>
<tr>
<td>Rollout #3: Fully implement CIS Control 2: Inventory and Control of Software Assets</td>
<td>(84.1)</td>
<td>1,892.7</td>
<td>$4.5M</td>
<td>$132.3M</td>
</tr>
<tr>
<td>Rollout #4: Fully implement CIS Control 4: Controlled Use of Admin Privileges</td>
<td>(90.0)</td>
<td>797.4</td>
<td>$3.7M</td>
<td>$121.7M</td>
</tr>
<tr>
<td>Rollout #5: Fully implement CIS Control 3: Continuous Vulnerability Management</td>
<td>(68.6)</td>
<td>575.8</td>
<td>$3.2M</td>
<td>$98.4M</td>
</tr>
<tr>
<td>Rollout #6: Fully implement CIS Control 5: Secure Config for HR and SLOM machines</td>
<td>(38.0)</td>
<td>289.6</td>
<td>$2.9M</td>
<td>$91.2M</td>
</tr>
<tr>
<td>Insurance: Transfer the risk into a cyber risk policy with $1M deductible and $15M limit</td>
<td>(26.0)</td>
<td>1,742.8</td>
<td>$2.0M</td>
<td>$54.4M</td>
</tr>
<tr>
<td>Total</td>
<td>(2,073.2)</td>
<td>8,321.6</td>
<td>$86.1K</td>
<td>$3.0M</td>
</tr>
</tbody>
</table>
Doing a Holistic Cyber Security Program – Quantified Cyber Risk

- Baseline Assessment
- Program / Roadmap
- Select and Implement Platform Solutions
- Operationalize to ensure Outcomes are Achieved
- Include Cyber Insurance
When designing the latest version of the CIS Controls, our community relied on 7 key principles to guide the development process.

1. Improve the consistency and simplify the wording of each sub-control
2. Implement "one ask" per sub-control
3. Bring more focus on authentication, encryption, and application whitelisting
4. Account for improvements in security technology & emerging security problems
5. Better align with other frameworks (such as the NIST CSF)
6. Support the development of related products (e.g. measurements/metrics, implementation guides)
7. Identify types of CIS controls (basic, foundational, and organizational)

https://www.cisecurity.org/blog/cis-controls-version-7-whats-old-whats-new/
Step 1 – Baseline Assessment

- Use surveys + internal automated assessment to test against CIS controls
- Compare survey response to automated testing
- Discuss differences
- Use sophisticated AI/ML modeling, with global threat data and breach impacts to Quantify Cyber Risks
Step 2 – Roadmap (3 year recommended)

- Program development (policies, procedures, controls mapping for compliance, etc.)
- Procure and implement tools
- Operations: Use a gap-based approach, get help with the areas you are not equipped to handle internally

- Prioritize initiatives based on actual economic impact to the business and how best to manage the economics of risks
- Provide actual costs for:
  - The Program
  - Platform/Tool + Implementation - taking into account the useful life of a solution including how to anticipate unknown threats and a phased plan based on identified priorities and risks.
  - Operations, Including IT, Security, and all applicable aspects of the business including the C-Level and Board.
  - Cyber Insurance at each level of maturity
Step 3 – Select and Implement Platforms / Tools

◆ Keep existing tools that help you achieve desired outcomes, replace those that don’t!

◆ Consider ecosystem

◆ Consider the full lifecycle of the platform / tool set

◆ Focus on achieving the outcomes defined in your Roadmap!
Step 4 – Operationalize

- Total Solution = People + Process + Technology
  - Expertise
  - Capacity
  - Core business
  - Transfer risk where appropriate (cyber insurance)
Is your cyber policy tied to actual risks or is it a “one-size-fits-all”?

Will your current policy actually cover a cyber incident?

A dynamic policy will change as your security posture changes

Policy should be tied to your roadmap
Example: Basic CIS Control 3 – Continuous Vulnerability Management

ADVERSARIES DON’T NEED MANY VULNERABILITIES ONE IS ENOUGH

Every

36 minutes
a new security vulnerability is identified*

That is an average of*

93 unique vulnerabilities per asset in the Financial industry

That is an average of

14,600 known and disclosed vulnerabilities each year*

It takes an average of

100 days
until known security vulnerabilities are remediated **

13 unique vulnerabilities per asset in the Healthcare industry

It takes

15 days on average for a vulnerability to be exploited**

7 unique vulnerabilities per asset in the Technology industry

* Nopsec: 2018 State of Vulnerability Risk Management
** Gartner Threat and Vulnerability Management Primer for 2017
Example: Basic CIS Control 3 – Continuous Vulnerability Management
Baseline Assessment

Survey says you do vulnerability management, automated assessment identifies vulnerabilities in your environment.

Discussion and program review reveals that while you have a scanning platform in place, it is difficult to keep up with remediation, and your program does not include strict SLAs and guidelines for classifying and remediating vulnerabilities.
Example: Basic CIS Control 3 – Continuous Vulnerability Management

Program Development

- Review and improve Vulnerability Management Program
- Define SLA (desired outcome) =
  - (using CVSS) No High or Critical vulnerabilities exist for more than 45 days
  - No medium vulnerabilities exist for 90 days
  - No Low vulnerabilities exist for 180 days
Operationalize the Program

- *Don’t have dedicated resources allocated to this task*
- *Don’t currently have enough resources to achieve these SLAs*
- *Only scanning quarterly, which doesn’t work for these SLAs*
- *Currently only performing patches for remediation*
- *No Sandbox in place for testing remediation*

Should you change the SLAs or how you do remediation?

Build a playbook that addresses these operational challenges.
QUESTIONS?
Next in our Webinar Series

... stay tuned for more cyber webinars. We are doing webinars on each of the CIS top 20 controls, and will release the first 3 scheduled webinars soon. Please call or send us a note, or follow us on LinkedIn and Twitter for more information.

Phone: +1 216-255-3040

Email: sales@asmgi.com

LinkedIn: https://www.linkedin.com/company/asmgi/

Twitter: https://twitter.com/ASMGi_CLE
Special Webinar Offer …

◆ … for those attending today’s webinar, please call +1 216.255.3040 or email Steve Roesing or Frank Yako directly for a NO COST Baseline Assessment.

sroesing@asmgi.com  fyako@asmgi.com

◆ We will perform the Baseline Assessment and review the results with you so that you fully understand how your quantified risk exposure looks today!

◆ This is especially meaningful if you are entering a budget cycle soon, as we will position you to base your budget request on real Quantified Cyber Risk and start building your Holistic Security Program immediately!
Thank You!

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Fax: 216.274.9647

Email: info@asmgi.com

www.asmgi.com