ASMGi

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 …

ASMGi

- **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

ASMGi

Total Solution = People + Process + Technology

A Holistic Approach to Cyber Security

ASMGi

Total Solution = 3 Pillars

Program Tech Operations

Way of thinking…

ASMGi

- **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

Way of thinking…

ASMGi

Way of thinking…

ASMGi

How Do You Make Decisions?

ASMGi

- **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 …

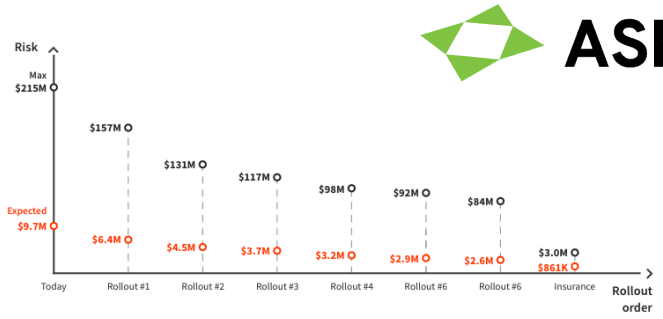
Quantifying Cyber Risk

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

Tower Street

- Dashboard
- Assets
- Health Check
- Vendors
- Reports

ASMGi



Recommendations (prioritized order)	Value Shift	Cost	Reduction in Expected Loss	Expected Loss
Today				Expected $0 (MIN) $ 9.7M $215M (MAX)
Rollout #1 Fully implement CIS Control 1: Inventory and Control of Hardware Assets	CIS #1 31% → 99%	(77.0)	3,262.3	$ 6.4M $157M
Rollout #2 Fully Implement CIS Control 1: Inventory and Control of Software Assets	CIS #2 36% → 99%	(78.1)	1,892.7	$ 4.5M $131M
Rollout #3 Fully Implement CIS Control 4: Controlled Use of Admin. Privileges	CIS #4 43% → 99%	(30.0)	797.4	$ 3.7M $117M
Rollout #4 Fully Implement CIS Control 3: Continuous Vulnerability Management	CIS #3 50% → 99%	(68.6)	575.8	$ 3.2M $98M
Rollout #5 Fully Implement CIS Control 5: Secure Config. for HW and SW on machines	CIS #5 38% → 99%	(30.0)	289.6	$ 2.9M $92M
Rollout #6 Fully Implement CIS Control 6: Mainten., Monitoring and Analysis of Audit Logs	CIS #6 53% → 99%	(24.5)	261.0	$ 2.6M $84M
Insurance Transfer the risk into a cyber risk policy with **$3M deductible** and **$100M limit**		(2,665.0)	1,742.8	$ 861K $3.0M
Total		(2,973.2)	8,821.6	

Doing a Holistic Cyber Security Program – Quantified Cyber Risk

ASMGi

- Baseline Assessment
- Program / Roadmap
- Select and Implement Platform Solutions
- Operationalize to ensure Outcomes are Achieved
- Include Cyber Insurance

Center For Internet Security - CIS Controls

ASMGi

CIS Controls™

V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

https://learn.cisecurity.org

7 Key Principles

When designing the latest version of the CIS Controls, our community relied on 7 key principles to guide the development process.

ASMGi

CIS Controls™

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

ASMGi

- 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)

ASMGi

- **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

ASMGi

- 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

ASMGi

- Total Solution = People + Process + Technology
  - Expertise
  - Capacity
  - Core business
  - Transfer risk where appropriate (cyber insurance)

Step 5 – Cyber Insurance

ASMGi

- 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

ASMGi

ADVERSARIES DON'T NEED MANY VULNERABILITIES ONE IS ENOUGH

Every

36 minutes

a new security vulnerability is identified*

It takes an average of

100 days

until known security vulnerabilities are remediated **

That is an average of*

93 unique vulnerabilities

per asset in the Financial industry

13 unique vulnerabilities

per asset in the Healthcare industry

7 unique vulnerabilities

per asset in the Technology industry

That is an average of

14,600 known

and disclosed vulnerabilities each year*

It takes

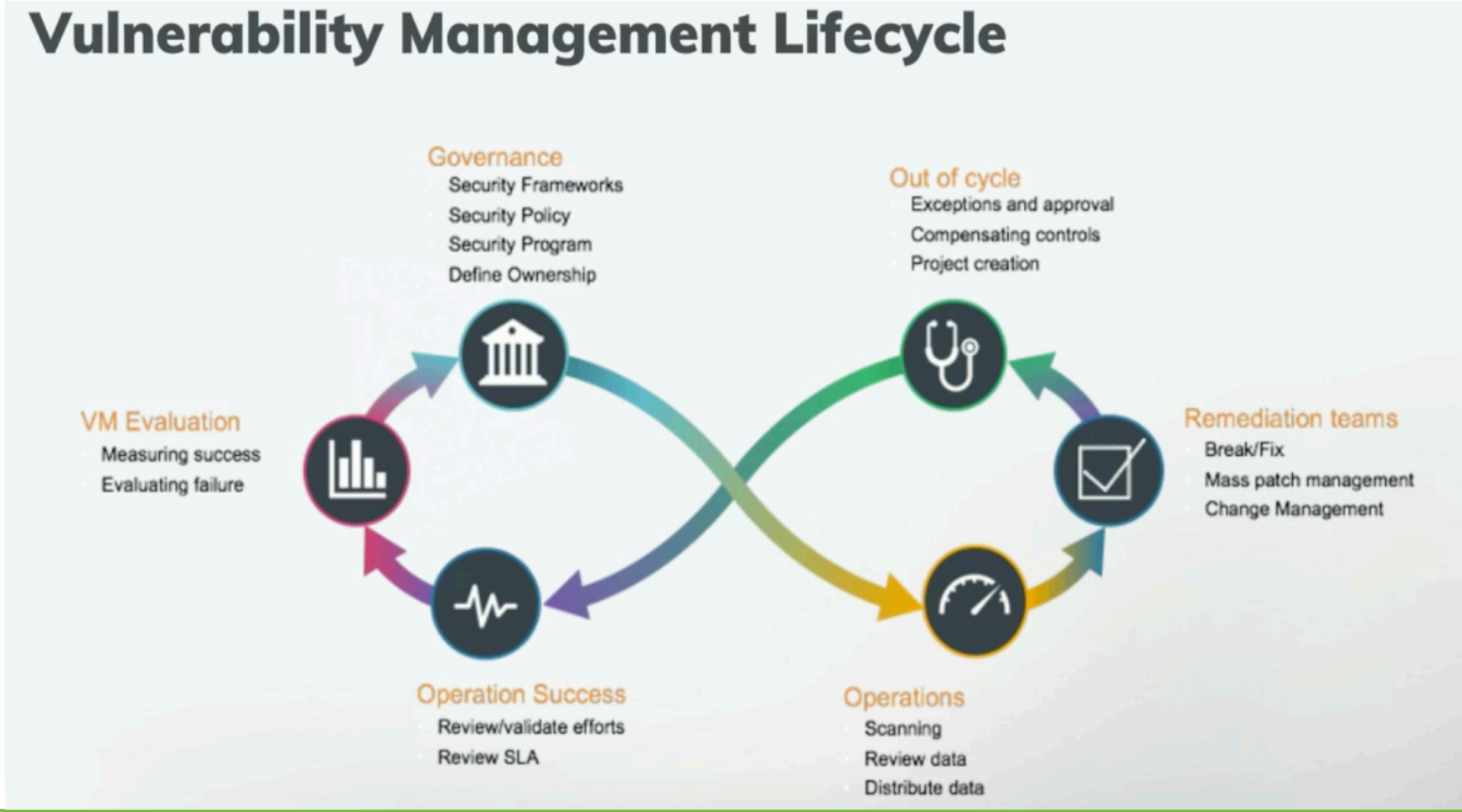
15 days

on average for a vulnerability to be exploited**

* Nopsec: 2018 State of Vulnerability Risk Management
** Gartner Threat and Vulnerability Management Primer for 2017

Example: Basic CIS Control 3 – Continuous Vulnerability Management

ASMGi



Example: Basic CIS Control 3 – Continuous Vulnerability Management

ASMGi

- **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

ASMGi

- **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***

Example: Basic CIS Control 3 – Continuous Vulnerability Management

ASMGi

- **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

ASMGi

… 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 …

ASMGi

- … 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!

ASMGi

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