ASMGi

Who Is Leading Your Cyber Security Program?

You Or Vendors?

Webinar Presented by ASMGi

March 28, 2019

Today's Webinar

Who Is Leading Your Cyber Security Program? You Or Your Vendors?

What does this mean? Three things, really …

1. The Technology / Tool is only part of the solution
2. Solution Vendors typically promise to solve your problem but only have visibility into the solution or problem their solution solves, yet often end up creating more work for you. We call this **focus on the problem** versus on the solution.
   - Ex: A scan report points out what is wrong, but it is still your job to make it right!
3. You are trying to solve a "business problem" (e.g. people, process, technology, policies, financial, etc.) where most vendors focus on the technology part of the "equation".

ASMGi is …

Global Technology Services and Consulting company focused on **Total Solutions** that provide immediate positive impact to your business

Total Solutions = People + Process + Technology

We deliver IT, Software and Cyber Security solutions from our headquarters in Cleveland, OH by helping our customers Plan, Manage and Execute:

- *Strong programs as a foundation to meet compliance requirements as well as foster best practices across the enterprise*
- *Best-in-Class platforms and tools to drive value thru adoption and shorter time to value*
- *A security eco-system model to ensure tools work together*
- *Achieve Results:*
  - ONEteam "XaaS" capabilities to ensure you maximize adoption – *Benefits without the Burden*!
  - "Fill the gap" approach to leverage your existing resources and complement/supplement where needed
  - Action = Results -> Orchestrated Action = Great Results!

Today's Presenters

Steve Roesing

President, CEO, ASMGi

Frank Yako

CIO, Director of Strategic Initiatives, ASMGi

Today's Agenda

- The Holistic Security Mindset
  - *Risk-Based approach*
  - *A holistic program is risk-based by default, because every decision has tradeoffs across the entire solution lifecycle to be considered*
  - *Total Solution = People + Process + Technology*
- The Vendor (or Point-Solution) approach
  - *Most vendors (OEMs) solve part of your problem (i.e., point solution)*
  - *Most vendors are motivated to "sell" or "solve" their portion of your solution, but what about the "Total" solution (are they creating more work for you?)*
  - *Most vendors want to help you succeed, as it relates to their portion of your solution*

How Do You Make Decisions?

- Point solution or holistic approach?
- Build roadmaps based on budgets or risk posture?
  - *Are you cost based or outcome based?*

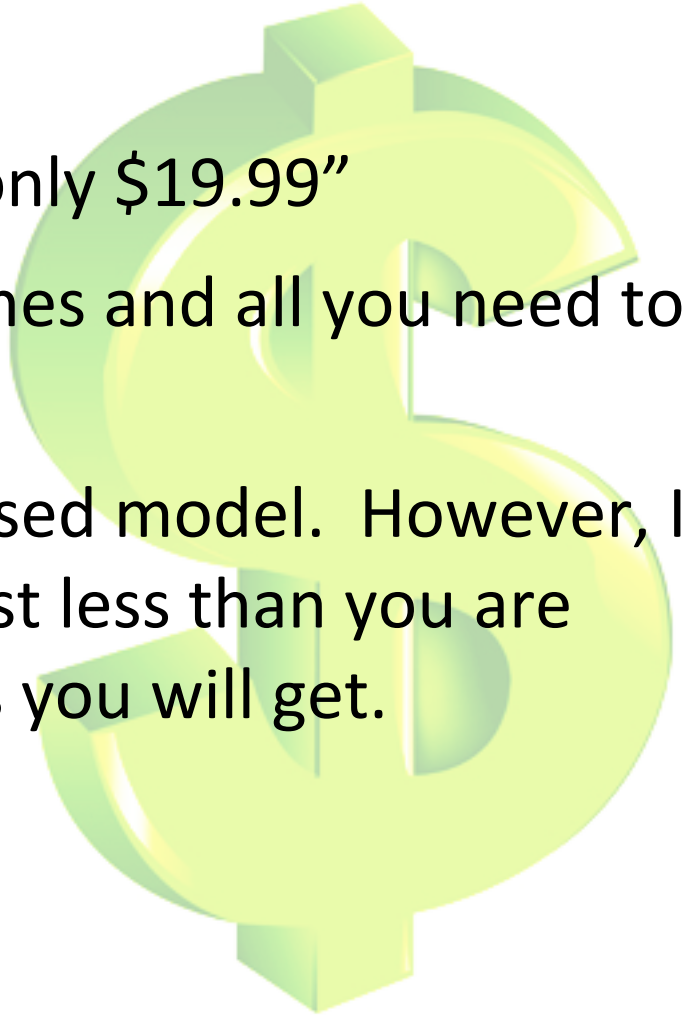
What If There Was A Way To Develop Your Program

Such That …

- The business understands what, when and why you are implementing solutions?
- You represent what an appropriate budget is for the enterprise, versus being told “how much” budget you’ll get to protect the organization
- Each implemented solution achieved a return on its own, AND worked well with current solutions and contributed to a larger eco-system (whole is greater than the sum of the parts)

There Is! You Can Have These Outcomes!

- It's not, and "You too can have all this for only $19.99"
- It's more like, "You CAN have these outcomes and all you need to do is think / act /do in a more Holistic way"
- This is a value-based model, NOT a cost-based model. However, I can tell you, with confidence, that it will cost less than you are spending now, and a fraction of the returns you will get.



A Couple Of Terms Often Cause Some Confusion

- Eco-system = The **IT ecosystem** is **defined** by Forrester Research and others as "the **network** of organizations that drives the creation and delivery of **information** technology products and services" and includes customers, suppliers, and influencers (key stakeholders).
- Budget driven versus outcome driven (cost-based versus value-based thinking)
- Orchestration: We have a saying that **Action = Results** -> It has evolved to **Orchestrated Action = Great Results!**
- Every vendor says their solution is best. How do you know which one to pick?
  1. *Ensure you have clearly defined objectives / problems you are trying to "solve" (Outcomes)*
  2. *Ensure you consider all elements of a Total Solution = focus on what outcome you want and make sure you are achieving that, not just one aspect of it.*
  3. *Ensure any new product fits into your ecosystem!*

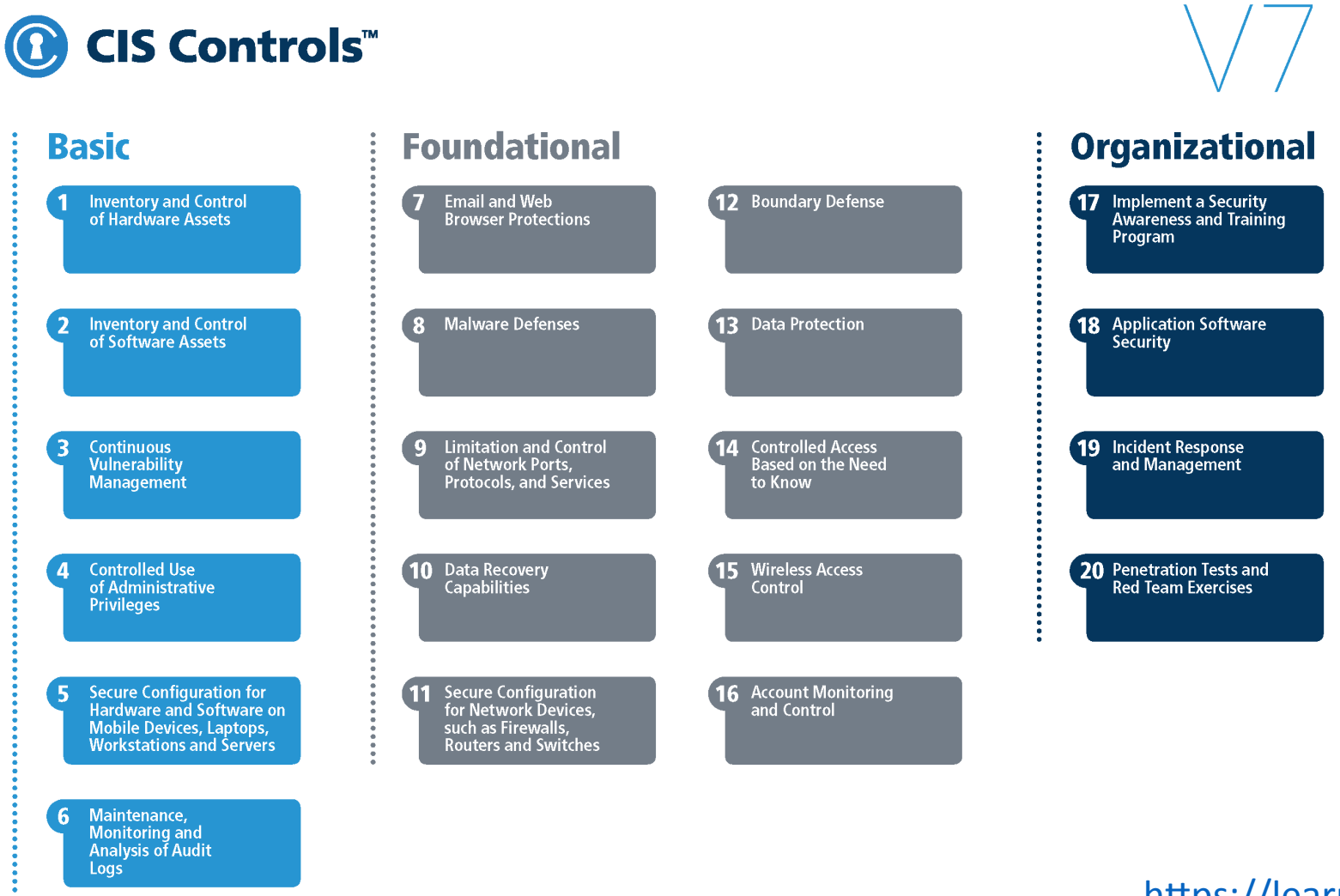
How Do you "Do" a Holistic Cyber Security Program

- Baseline Assessment
  - *Including an assessment of your current cyber portfolio and investments*
  - *Represent Quantified Results*
- Program / Roadmap
  - *Including defining your desired outcomes*
- Select and Implement platform solutions
- Operationalize to ensure outcomes are achieved
  - *Demonstrate through measurement*
  - *Include Cyber Insurance*

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
- ***Quantifying Cyber Risk - Why is it important***
  - *Bring security closer to the business*
  - *Create a common language to discuss cyber risks*
  - *Prioritization = Align budgets with initiatives that provide actual economic impact*

Center For Internet Security - CIS Controls



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.

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 2 – Roadmap (3 year recommended)

- 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
- Develop programs
- Procure and implement tools
- Perform operations
- Gap-based approach, meaning we fill whatever gaps exist in your ability to fully execute the Plan
- Program development (policies, procedures, controls mapping for compliance, etc.)
  - Could or should include preparation for annual audits, reporting, etc.
- Technology partners / eco-system
- Expertise / People resources to fully operationalize

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
- Leverage Cyber Insurance where appropriate

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*

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*

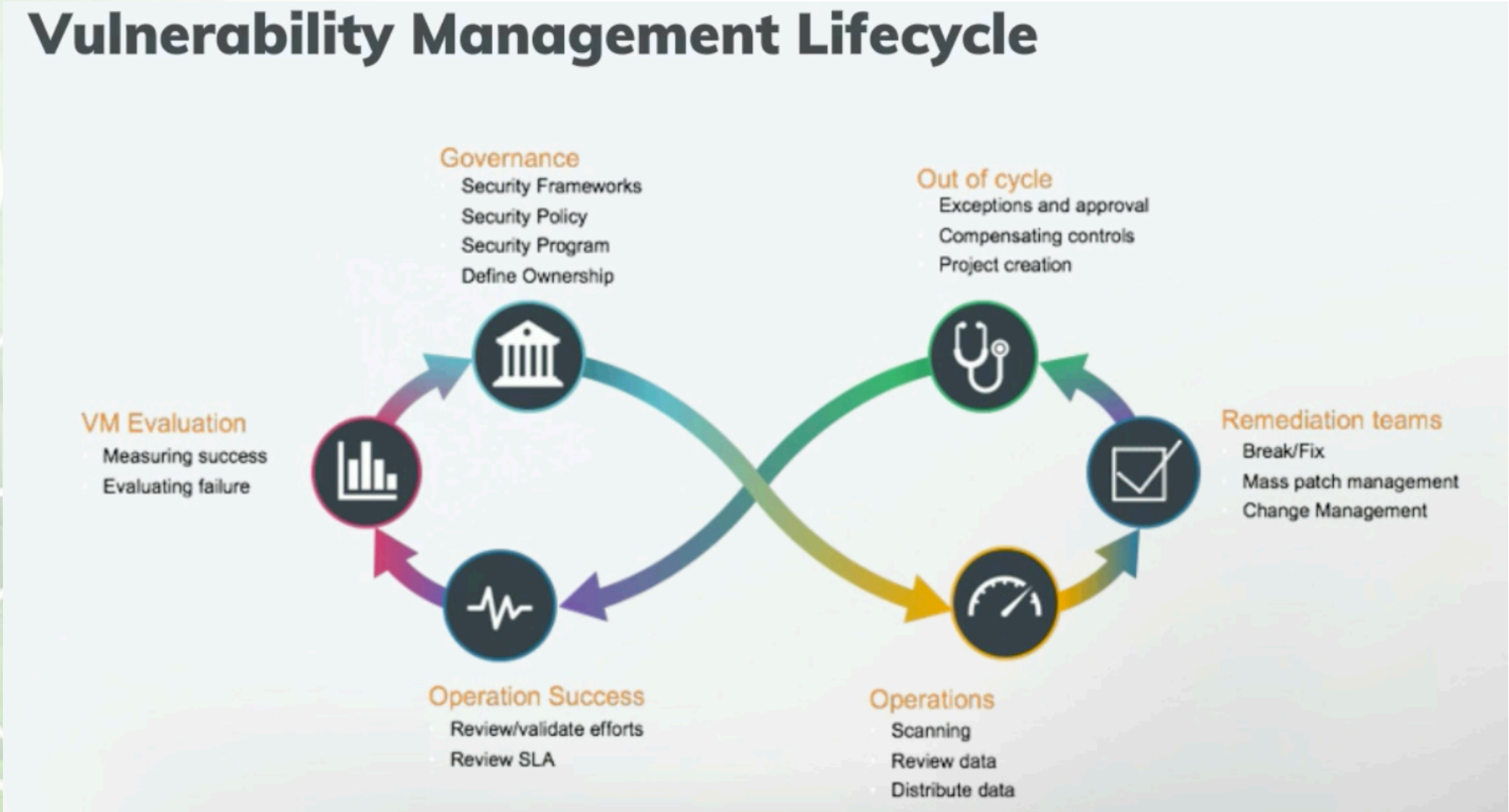
It takes

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



Example: Basic CIS Control 3 – Continuous Vulnerability Management

- Baseline Assessment
  - *Survey says you do vulnerability management, automated assessment identifies vulnerabilities in your environment*
  - *Discussion reveals that you 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

- Holistic Solution
  - *Review and improve Vulnerability Management Program*
  - *Define SLA (desired outcome) =*
    - (using CVSS) No High or Critical vulnerabilities exist for more than 60 days
    - No Medium vulnerabilities exist for 120 days
    - No Low vulnerabilities exist for 180 days

Example: Basic CIS Control 3 – Continuous Vulnerability Management

- Operationalize the Program
  - *Don't have dedicated resources allocated to this task*
  - *Don't currently have enough resources to achieve these SLAs*
  - *Don't have dedicated resources allocated*
  - *Don't have enough resources to achieve the 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

Future-Ready Datacenter, Future-Ready Managed Services
The Five Things You Need to Know Right Now

Presented by ASMGi and Flexential, on Thursday April 11, 2019 l 1-2 PM ET

Managed Services experts from ASMGi and Colocation Experts from Flexential will discuss the top five things to understand about managed colocation services including:

- Improved security and business continuity
- Proactive approach to IT problems and improved uptime
- Easier access to newer technologies and trends – Edge Computing / Hybrid IT
- Cost savings and avoidance
- Migration to private or public cloud solutions

Visit www.asmgi.com Resources page to sign up

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