Security Leaders:
Manage the Forest
Not the Trees

Presented by:
Adam Stone
Secure Digital Solutions, LLC
15 March 2018 | 2:50 pm
Your Facilitator

Adam Stone

Principal Consultant and Chief Privacy Officer

Secure Digital Solutions, LLC

Over 28 years business leadership

18+ years experience in data security and privacy strategy and program development

Focused in performance management, policy, strategy and corporate stewardship

Certified FIP (Fellow in Information Privacy), CIPP, CIPM, CISSP-ISSMP, HCISPP, CHPS
Disclaimer

The views expressed in this presentation do not necessarily reflect the views of Secure Digital Solutions, LLC.

This presentation is for informational purposes only. The content of this presentation does not constitute legal advice and should not be interpreted as such. Secure Digital Solutions, LLC is not a law firm. Consult a qualified attorney for questions pertaining to compliance with US or international law.
Today’s Topics

Part I | Managing Perception
Part II | Measurement Techniques
Part III | Cybersecurity Maturity
Summary | Wrap Up
Managing Perception
Part I
"All credibility, all good conscience, all evidence of truth come only from the senses."

- Friedrich Nietzsche, *Jenseits von Gut und Böse (Beyond Good and Evil)*
Basic Truths About Today’s Security Leaders

Security Leaders Need Metrics to Communicate Effectiveness

Senior Stakeholders Seek Trust and Confidence

Security Leader Struggles to Effectively Communicate to Senior Stakeholders

Senior Stakeholders Struggle to Understand Value of Cybersecurity

Security Leaders’ Credibility Suffers as a Result of Mismatched Expectations

Cybersecurity Function Left Underfunded and Underappreciated
How Do Security Leaders Want to be Perceived?

**Business Hinderance**
- Feared or off-putting.
- Manager of “You Can’t.”
- Overtly tactical.
- Flagging credibility among organizational leadership.

**Business Enabler**
- Respected by peer-functions.
- Opportunity-seeking.
- Overtly strategic.
- High confidence among organizational leadership.
Perception is Everything.
The Security Leader’s Aspirations

THE FOUR FACES OF THE CISO
CURRENT STATE

Guardian 41%
Technologist 33%
Strategist 15%
Advisor 12%

THE FOUR FACES OF THE CISO
DESIRED STATE

Advisor 35%
Strategist 32%
Guardian 22%
Technologist 12%
Identifying a Key Business Problem

Communication Breakdown:
Executives and security leader speak different languages.

Communications tend to focus on trees; not the forest.

Where did my credibility go?
What Does Management Expect?

EXECUTIVES: HOW DO YOU PREFER INFORMATION REGARDING CYBERSECURITY BE PRESENTED?

- High-level security strategy descriptions: 33%
- Risk metrics: 31%
- Security and risk posture compared to peers: 11%
- Description of security technologies: 11%
- I am not regularly briefed on security posture: 4%
- Audit and compliance status: 9%
- Anecdotes: 1%

Copyright © 2018 Secure Digital Solutions, LLC | All rights reserved.
Whenever cyber[security] is raised there is technical devolution... Immediately, directors jump to management and executive level issues, and not board issues.

Confidence Among Management

EXECUTIVES: HOW CONFIDENT ARE YOU THAT YOUR COMPANIES ARE PROPERLY SECURED AGAINST CYBERATTACKS?

- Confident: 29%
- Very Confident: 4%
- Less Than Confident: 67%
In Summary...

Security leaders need to measure cybersecurity performance.

Security leaders aspire to be a trusted advisor.

Security leaders need a better way to communicate business-value to executives and board members.
Measurement Techniques

Part II
Comparison: Cybersecurity Measurement Techniques

<table>
<thead>
<tr>
<th>Maturity</th>
<th>Strategic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>Probabilistic</td>
</tr>
<tr>
<td>Compliance</td>
<td>Binary</td>
</tr>
<tr>
<td>Controls</td>
<td>Granular</td>
</tr>
<tr>
<td>Ad Hoc</td>
<td>Arbitrary</td>
</tr>
</tbody>
</table>
# Cybersecurity Measurement Techniques

<table>
<thead>
<tr>
<th>Measurement Technique</th>
<th>Objectives</th>
<th>Goals</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad Hoc Assessment</td>
<td>Measure cybersecurity effectiveness whenever convenient.</td>
<td>Spend as little time as possible measuring cybersecurity effectiveness.</td>
<td>Helps free up time to respond to the endless series of fire calls and other catastrophes.</td>
</tr>
<tr>
<td>Controls Assessment (Audit)</td>
<td>Comply with prevailing reporting requirements.</td>
<td>Seek evidence that an organization implements and adheres to its internal policies and controls.</td>
<td>Provide assurances by aligning business practices with internal policies and controls requirements.</td>
</tr>
<tr>
<td>Compliance Assessment</td>
<td>Comply with prevailing legal and regulatory obligations.</td>
<td>Seek evidence that an organization implements and adheres to its legal and regulatory obligations.</td>
<td>Reduce exposure by aligning business practices with compliance requirements.</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Manage risk to an acceptable level.</td>
<td>Identify and prioritize risks based on an analysis of threats, vulnerabilities and mitigating controls factored against the likelihood that a threat actor will exploit a given vulnerability.</td>
<td>Enable organizations to predict and prepare security defenses for future loss events.</td>
</tr>
<tr>
<td>Process Maturity Assessment</td>
<td>Manage organizational accountability of processes to improve performance.</td>
<td>Measure the capacity to effectively and efficiently manage an information security program.</td>
<td>Enable organizations to improve security-related business processes by motivating a culture of security throughout.</td>
</tr>
</tbody>
</table>
Ad Hoc **Measurement**

Little up-front work needed.

No dependencies mapped.

Treats cybersecurity as a (potentially chaotic) mass of solutions to problems, as they pop up.

*Not a recommended measurement technique!*
Measuring and Managing Cybersecurity by Controls

Better understood by operational/technical folks.

Easily aligns with supporting technologies.

Treats and measures specific activities granularly, by delving into the particulars of a given control.

Useful for auditing and measuring compliance or risk.
Example: Controls-Based Measurement (1)
Example: Controls-Based Measurement (2)

Average Score = Medium-Low

1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 + 11 + 12 + 13 + 14
Example: Risk-Based Measurement

Average Score = Medium-Low Risk
Example: Compliance-Based Measurement

In compliance = 6 (43%)
Not in compliance = 8 (57%)
Measuring and Managing Cybersecurity by Process

Better understood by non-technical folks.

Easily aligns with supporting functions and processes.

Treats and measures specific activities holistically, by considering people, process, and technology.
Example: Process-Focused Measurement (1)
Example: Process-Focused Measurement (2)

Average Category Score = Medium
Example: Process-Focused Measurement (NIST CSF)

Win!
Security Leader as Communications Bridge

Security Leader

- Strategic-Focus
  - Business Drivers, Needs, and Expectations

- Process-Focus
  - Security Strategies

- Controls-Focus
  - Security Operations

Copyright © 2018 Secure Digital Solutions, LLC | All rights reserved.
Parts of a Comprehensive Security Program
In Summary...

Measurement techniques vary by objectives, goals and benefits.

Effective security leaders serve as a communications bridge between operations and management.

Most effective measurement strategies treat security as a comprehensive program with its own subspecialties, tools, and processes.
Cybersecurity Maturity
Part III
Defining Cybersecurity “Maturity”

What does this concept mean to you?
“Maturity

The state of being mentally and emotionally well-developed, and therefore responsible.

The state of being fully grown or developed.

- Oxford Advanced Learner’s Dictionary and Merriam-Webster Dictionary, respectively
## Characteristics of High and Low Maturity

<table>
<thead>
<tr>
<th>High Maturity (Participant Input)</th>
<th>Low Maturity (Participant Input)</th>
</tr>
</thead>
<tbody>
<tr>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>•</td>
<td>•</td>
</tr>
</tbody>
</table>
Effects of High and Low Maturity

**High Maturity**
- Security as **strategic advisor** to executives.
- Security as **business-enabler**.
- Security as **performance leader** (highly developed and sustainable).

**Low Maturity**
- Security as **firefighter** and **tactical expert**.
- Security as a **barrier to business growth and profitability**.
- Security as a **pure cost** to the business.

How is the cybersecurity leader/function perceived by the organization?
Effects of High and Low Maturity

How is the cybersecurity leader/function perceived by the organization?

Let me show you how the maturity of our cybersecurity program adds value to the business!

We’ve got a bunch of cybersecurity controls to protect stuff. I shall now give you all the gory details!
Industry Definitions of “Maturity” (1)

Many maturity models and definitions developed over the years:

- Organizational Project Management Maturity Model (OPM3®)
- Portfolio, Programme, and Project Management Maturity Model (P3M3®)
- PRINCE2® Maturity Model (P2MM®)
- Capability Maturity Model Integration (CMMI®)
Industry Definitions of “Maturity” (2)

Key cybersecurity guidelines now use “maturity” as part of the scoring methodology, such as:

- FFIEC Cybersecurity Assessment Tool (CAT)
- COBIT®

Cybersecurity solutions providers now use the word “maturity” to promote the benefits of products and services.

Often, “maturity” is used without a formal definition.

“Maturity” is usually intermingled with the notion of “risk” management or assessments.
Tips for Understanding Cybersecurity Maturity

Best used to assess business processes, not specific controls.

Focused on several attributes or dimensions, each providing a rich set of data points.

Cybersecurity maturity is not synonymous with risk.
Cybersecurity Process Maturity: Industry Adoption

No commonly-accepted definition (yet) of “maturity” used by security leaders.

Cybersecurity “maturity” often confused with the definition of cyber “risk.”

These terms (maturity and risk) have different connotations and uses.

The scales used to define varying levels of cybersecurity “maturity” differ.
### Example: Maturity Attributes (or Dimensions)

<table>
<thead>
<tr>
<th>Processes</th>
<th>Awareness</th>
<th>Policy</th>
<th>Automation</th>
<th>Expertise</th>
<th>Accountability</th>
<th>Measurability</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID.AM</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>ID.BE</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>...</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>...</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>
# Example: Assessing Cybersecurity Maturity

### Cybersecurity Maturity

<table>
<thead>
<tr>
<th></th>
<th>Baseline</th>
<th>Evolving</th>
<th>Intermediate</th>
<th>Advanced</th>
<th>Innovative</th>
</tr>
</thead>
<tbody>
<tr>
<td>We tend to treat security as an IT subject.</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Our cybersecurity oversight tends to focus on past event (such as an incident).</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>We receive filtered cybersecurity information from management.</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Information about emerging cyber threats is filtered through the CEO before coming to the Board.</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>We tend to treat cybersecurity as an enterprise risk.</td>
<td></td>
<td></td>
<td></td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Cybersecurity is part of our forward-looking discussions with management.</td>
<td></td>
<td></td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>We receive unfiltered cybersecurity information from management and experts.</td>
<td></td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
<tr>
<td>Information about emerging cyber threats is discussed openly, with no CEO filtering, by the Board.</td>
<td></td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
<td>![ ]</td>
</tr>
</tbody>
</table>
In Summary...

Cybersecurity process maturity focuses on the forest, while minding the trees.

When used as a key performance indicator (KPI), maturity is what organizations make of it.
Presentation Summary and Final Thoughts

Disconnect between stakeholder expectations and operational realities (despite best efforts).

Credibility takes a hit when security leader/function perceived as an extension of IT operations.

Bridge the communications gap by elevating the focus from controls to process.

Metrics focused on process “maturity” offer promising tools for improving communications.
Thank You for Your Participation!

Adam Stone
Principal Consultant and Chief Privacy Officer
Secure Digital Solutions, LLC
astone@trustsds.com
952-544-0234