Assess and Mature your Cybersecurity Program Today

October 10, 2023
**Today’s Speakers**

*IT Risk, Process, Cybersecurity and Digital Transformation Expertise*

---

**Carl Grifka**
Managing Director, CISSP, CISM, CISA, PMP, CDPSE

Managing Director of SL Business Informatics
Prior experience includes Top 10 CPA firm Risk Consulting Director, Private and Public sector IT auditor; Global enterprise CFO
Frequent speaker and nonprofit board member
SLBI Practice areas - IT Risk, Internal Audit, Cybersecurity, SOC Reporting, BC/DR Planning, Project Management

**Eric Rockwell**
Lead Cybersecurity Advisor, CISSP, vCISO

Former in-house IT executive roles: CEO and CISO
Frequent speaker (Cybersecurity risk management)
Author of American Bar Association Information Security Policy Handbook
Contributor to the Center for Internet Security (CIS) Controls v8.0
Leads Cybersecurity and risk assessments, Information security programs, monitoring and oversight
Learning Objectives

- What a Cybersecurity “program” is – and how Management is involved
- How the cybersecurity program can be used to assess, identify and manage material risks from Cybersecurity threats
- How management can oversee risks from Cybersecurity threats.
- How material incidents may need to be disclosed by the participant’s company and the required timing.

Reviewed in the context of the new SEC Cybersecurity disclosure rules published on July 26, 2023
Polling Question #1

What function do you represent within your company?

A. Audit
B. Cybersecurity
C. Risk Management
D. IT
E. Finance
F. Other
Cybersecurity is a continuous living process of maturity and risk management

You have to start somewhere

You should assess and measure your progress

It involves on-going assessment of your Cybersecurity maturity and capabilities – and remediating, designing and improving your posture

If you already are deploying or managing a cybersecurity program, GREAT! But - do you objectively measure your program and improve it on an ongoing basis?
A Cybersecurity Program

What is a Cybersecurity Program?
The formal, auditable, measurable activities undertaken to manage Cybersecurity risks and threats.

Who is responsible for a Cybersecurity Program?
Cybersecurity management is an element of IT Governance - which is a management responsibility (read: not only IT).

What is IT Governance?
IT governance is defined as the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals. IT demand governance (or "ITDG" - what IT should work on) is the process by which organizations ensure the effective evaluation, selection, prioritization, and funding of competing IT investments; oversee their implementation; and extract (measurable) business benefits. ITDG is a business investment decision-making and oversight process, and it is ultimately a business management responsibility. (Gartner)

SL emphasis: Cybersecurity is one – of many things – that IT “works on”
Information Technology goals differ from Information Security goals.

There is a need to manage these conflicting viewpoints internally.
The 3 definitions aggregate several vital themes to the deployment of Cybersecurity:

- “People”
- Origination: Outside and Inside
- Purpose of Cybersecurity: “ensure availability, integrity, authentication, confidentiality, and nonrepudiation” of your digital information

The term: “Practice”...
Are all Cybersecurity Programs the same?

- No
- Why?
- How they differ
- Illustrations
Security Maturity Levels: How does your organization stack up?

Initial (1.0)
- Activities unstaffed or uncoordinated
- No formal security program in place
- Information security (Infosec) leadership established, informal communication
- Basic governance and risk management process, policies
- Some controls in development with limited documentation

Developing (2.0)
- Increased resources and awareness, clearly defined roles and responsibilities
- Organization-wide processes and policies in place but minimal verification
- Formal infosec committees, verification and measurement processes
- More controls documented and developed, but over-reliant on individual efforts

Defined (3.0)
- Increased resources and awareness, clearly defined roles and responsibilities
- Organization-wide processes, policies and controls in place, but minimal verification
- Controls monitored, measured for compliance, but uneven levels of automation

Managed (4.0)
- Increased resources and awareness, clearly defined roles and responsibilities
- Formal infosec committees, verification and measurement processes
- Controls monitored, measured for compliance, but uneven levels of automation

Optimized (5.0)
- Culture supports continuous improvement to security skills, process, technology
- Processes more comprehensively implemented, risk-based and quantitatively understood
- Controls more comprehensively implemented, automated and subject to continuous improvement
Polling Question #2

Based on your knowledge, what maturity level is your company’s cybersecurity Program at today?

A. 1 - Initial
B. 2 - Developing
C. 3 - Defined
D. 4 - Managed
E. 5 - Optimized
F. I’m not sure
A path to manage Cybersecurity:

We recommend a 12-step Managed Information Security Program

01 Conduct a Security Maturity Level Assessment (SMLA)
02 Form Information Security Committee
03 Write and Approve Information Security Policies and Procedures
04 Undertake Security Policy and Employee Awareness Training
06 Compliance Portal Goes Live
07 24/7/365 Security Operations Center (SOC) (ongoing alert monitoring, investigation and escalation)
08 Ongoing Vulnerability Management and Remediation
09 Intrusion Detection and Data Loss Prevention Software Implemented
10 Create Incident Response Plan
11 Review and Approve Cyber Liability Insurance Policy
12 Penetration Testing

Today we will focus on the periodic security maturity level assessment (SMLA) – Step 1
Elements of Cybersecurity: NIST Cybersecurity Framework (CSF)

- **Identify**
  - Asset Management
  - Business Environment
  - Governance
  - Risk Assessment
  - Risk Management Strategy

- **Protect**
  - Access Control
  - Awareness and Training
  - Data Security
  - Info Protection Processes and Procedures
  - Maintenance
  - Proactive Technology

- **Detect**
  - Anomalies and Events
  - Security Continuous Monitoring
  - Detection Processes

- **Respond**
  - Response Planning
  - Communication
  - Analysis
  - Mitigation
  - Improvements

- **Recover**
  - Recovery Planning
  - Improvements
  - Communications

**PROACTIVE**

**REACTIVE**
We recommend that organizations perform a Security Maturity Level Assessment (SMLA), which is a periodic evaluation of the progression and capability of their cybersecurity program, with a view to creating effective, repeatable security processes to be improved continuously. The security maturity level of an organization is represented by an indicative score, which can be improved through recommended actions.

**Continuous reperformance and evaluation to improve maturity levels over time**
We recommend the use of the Center for Internet Security (CIS) framework within a SMLA assessment. Simply put, the CIS framework is a holistic set of standard security controls that you can use to measure and enhance your IT environment over time. CIS is the approved implementation plan for the NIST CSF, the standard source for insurance questionnaires, and is mapped to major cybersecurity frameworks. Leveraging the CIS framework is a solid starting point and is in our opinion the best overall source of cybersecurity controls to measure and improve your security program.

**CIS Control Domains**

CIS Control 1: Inventory and Control of Enterprise Assets
CIS Control 2: Inventory and Control of Software Assets
CIS Control 3: Data Protection
CIS Control 4: Secure Configuration of Enterprise Assets and Software
CIS Control 5: Account Management
CIS Control 6: Access Control Management
CIS Control 7: Continuous Vulnerability Management
CIS Control 8: Audit Log Management

CIS Control 9: Email and Web Browser Protections
CIS Control 10: Malware Defenses
CIS Control 11: Data Recovery
CIS Control 12: Network Infrastructure Management
CIS Control 13: Network Monitoring and Defense
CIS Control 14: Security Awareness and Skills Training
CIS Control 15: Service Provider Management
CIS Control 16: Application Software Security
CIS Control 17: Incident Response Management
CIS Control 18: Penetration Testing
SMLA Key Deliverables

Executive Summary
Document to review findings, remediation recommendations and roadmap, and respond to questions.

Security Maturity Level Report
Based on the findings, your organization should develop a security maturity report based on the CIS Controls and NIST CSF Mapping. The organization should determine its maturity score between 0 – 5.

IT Security Roadmap and Budget
The organization should develop a roadmap to achieve a phased remediation path and allocate budget to achieve the target security maturity level. These typically run between 3 – 12 months.
Polling Question #3

Does your company conduct a regular periodic cybersecurity maturity level assessment (e.g., SMLA type of exercise)?

A. Yes, every year
B. Yes, every couple of years
C. No, we do not do this regularly
D. I’m not sure
Contemplation: Assessing your Cybersecurity Risks

- Is information security risk management important to your business?
- What is being done, presently, to manage this risk? How much is being spent on it?
- Who is managing it, and who are they accountable to?
- Do you trust that it’s being managed competently?

Risk Assessment “101” -
- What are the risks and threats to your digital assets?
  Then for each risk/threat, assess:
- What is the impact should any of the risks and threats occur?
- What is likelihood of occurrence?
Polling Question #4

Does your company conduct a regular periodic cybersecurity risk assessment?

A. Yes, every year
B. Yes, every couple of years
C. No, we do not do this regularly
D. I’m not sure

These new disclosures cover cybersecurity program strategy, risk management, governance, and incident response.

What’s at stake? In short – it’s time to disclose how your organization governs and manages material cybersecurity risks, threats and incidents – as well as disclosure of material cybersecurity incidents.

How soon? For many filers, these rules apply as early as fiscal years ending after 12/15/23.
Cyber incident reporting: material incidents need to be disclosed (typically) within 4 business days; specifically, the nature, timing, and material impact or reasonably likely material impact on the organization. (Disclosed on Form 8-K)

Cyber risk management: how you assess, identify and manage material risks from Cybersecurity threats – and determine how possible and previous incidents can impact your organization. (Disclosed on form 10-K for domestic registrants, Regulation S-K)

Cyber governance: your board’s oversight of risks from Cybersecurity threats – and your management’s role and expertise in addressing material risks from Cybersecurity threats. (Disclosed on Form 10-K for domestic registrants, Regulation S-K)
A Path to Meet SEC Requirements

To prepare for these complex SEC disclosure requirements, we recommend that public company registrants perform the following actions:

1. Evaluate the readiness of your cybersecurity program for SEC disclosure compliance.
   - We recommend completing a SMLA with an added focus on incident response and recovery to understand the risks/threats that may impact your business and to assess your IT security processes and controls.

2. Develop a SEC Cybersecurity compliance roadmap for remediation of policies, controls, governance and behavior.
   - Implement critical items ASAP for compliance and other roadmap improvements over time.

3. Ensure that your management team and your Board understand their oversight responsibility in the management of Cybersecurity risks and threats.
   - Consider education and training to remediate any gaps in knowledge.

Skillsets needed

Subject Matter Professionals

- **Role 1**
  Hands-on, skilled Cyber and SEC accounting technical support to establish processes designed to help build your capability to comply with these rules.

- **Role 2**
  Seasoned, skilled Cyber and SEC accounting eyes to assess your compliance posture.
Polling Question #5

What is the primary challenge to implement or maintain a cybersecurity program at your organization?

A. Conflicts of goals between IT operations and cybersecurity
B. Budget or cost constraints
C. Lack of Management buy-in based on their understanding of the risk
D. Lack of time or staff expertise needed to support the program
E. We do not have any challenges maintaining a cybersecurity program
F. I’m not sure
Practical Challenges of Cybersecurity

✓ Cyber solved by IT or Behavior?
✓ Tone at the top
✓ Formality of controls, policies, enforcement, consequences
✓ Balancing morale, efficiencies, security, protection
✓ Use of AI and machine learning
✓ Dangers of Cyber being seen as a one-time exercise
✓ Continuously changing regulatory environment
You may be in a governance, IT or risk management position

Risks vary among all businesses; impactful and likely risks require attention – particularly those to your sensitive digital assets

Your role is to govern the implementation of a Cybersecurity Program to manage the risks you deem worthy of mitigating

This Program is an on-going series of maturation activities whose effectiveness is measured over time (e.g., with a SMLA)

Cyber protection is very much about both your IT organization and your company’s Management team – without them you can’t protect your data

We are here to help
Thank You!

If you have questions or want to follow up – let us know – we’re here to help.

Carl Grifka, CISSP, CISA, CISM, PMP, CDPSE
Managing Director, SL Business Informatics
+1.248.266.0839
Carl.Grifka@SingerLewak.com

Eric Rockwell, CISSP, vCISO
Cybersecurity Lead, SL Business Informatics
+1.619.514.7350
ERockwell@SingerLewak.com

Singerlewak.com
SLBusinessInformatics.com
Foresight-SLBI.com (digital transformation advisory)