scottmadden
MANAGEMENT CONSULTANTS

Smart. Focused. Done Right.®

Strategic Cybersecurity

A Toolkit for Prioritizing, Coordinating, and Transforming Your Cybersecurity Program

Strategic Cybersecurity: A Toolkit for Prioritizing, Coordinating, and Transforming Your Cybersecurity Program

If your company is like most, cybersecurity has become both a priority and a source of frustration:

- Cyber risks are real and have the potential to be destructive to your organization’s ability to provide service to your customers
- Yet, the efforts to address these risks often seem to have their own negative business impacts
  - They are expensive
  - They hurt productivity
  - Their success is difficult to measure

Rather then continue to throw money at cybersecurity and hope that nothing bad happens, energy providers must pursue an alternative approach:

- A more business-like approach to identifying cyber risks and the appropriate response to these risks
- An approach aligned with industry guidance and expectations to demonstrate appropriate diligence and rigor given today’s environment
- An approach that establishes desired outcomes and measures progress against these outcomes

This report describes a strategic approach to cybersecurity that engages both security professionals and business stakeholders in order to:

- Answer four critical questions to establish the direction of their cybersecurity programs
- Implement a cybersecurity program consistent with this direction
- Sustain and continuously improve program performance based on key program performance indicators

This approach will help you target your most important enterprise risks and gain confidence in the ability of your cybersecurity program to protect your critical assets.

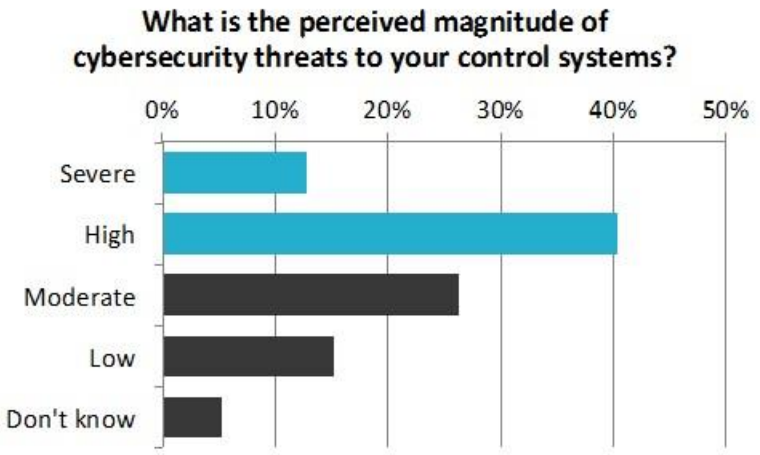
scottmadden
MANAGEMENT CONSULTANTS

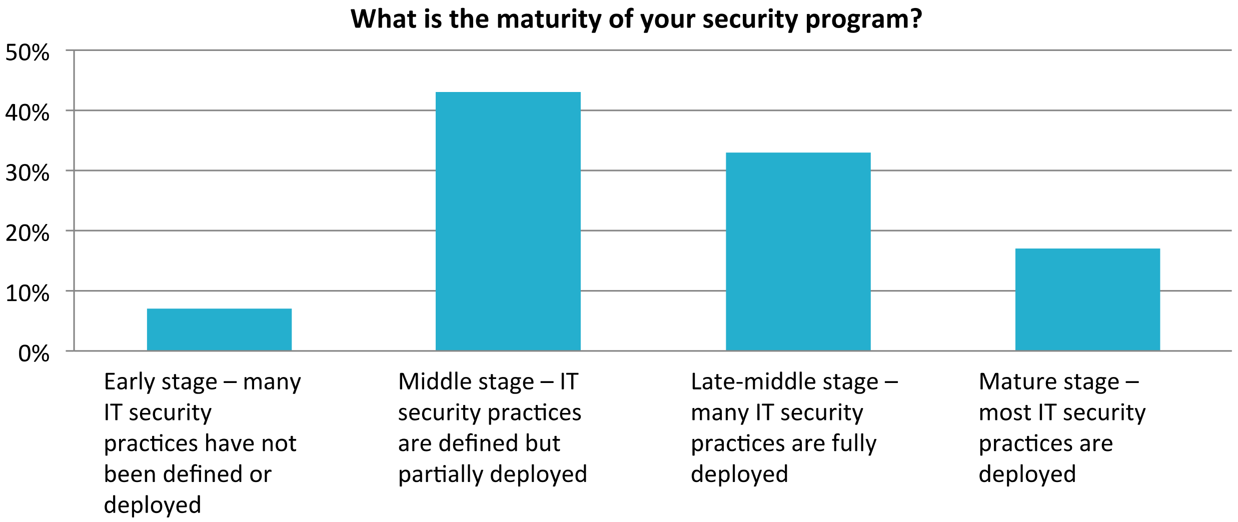
Energy Organizations Are Aware of Significant Cyber Threats and Are Investing in Efforts to Manage Their Risks

Electric utilities' core mission remains the same—delivering safe, reliable power to customers, but a new class of risks threatens this mission. Cyber risks have the potential to impair power-producing assets and their ability to deliver critical services to customers.

The industry is responding. In ScottMadden's annual Energy Industry Cybersecurity Report, we identified the following key findings:

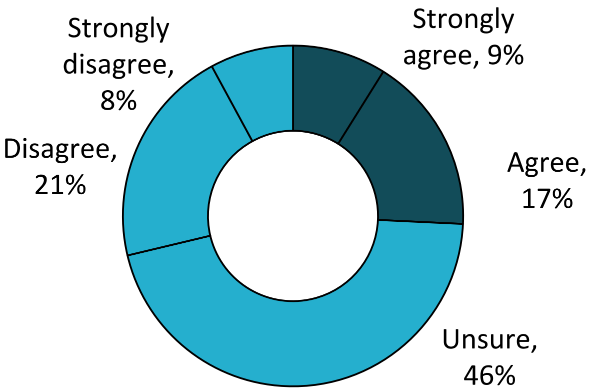
- Energy organizations acknowledge a growing cybersecurity risk and most expect their IT and Operation Technology (OT) assets to be attacked
  - More than 50% categorized cybersecurity threats as either high or severe
  - Most organizations have experienced a cybersecurity incident that resulted in either a data loss or disruption to operations
- In response, most organizations have implemented cybersecurity programs and consider their programs to be relatively mature



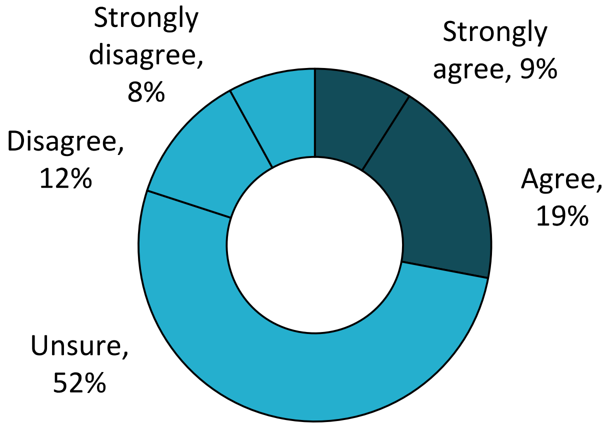


Despite These Efforts, Energy Leaders Are Not Confident That They Are Really Improving the Security of Their Critical Assets

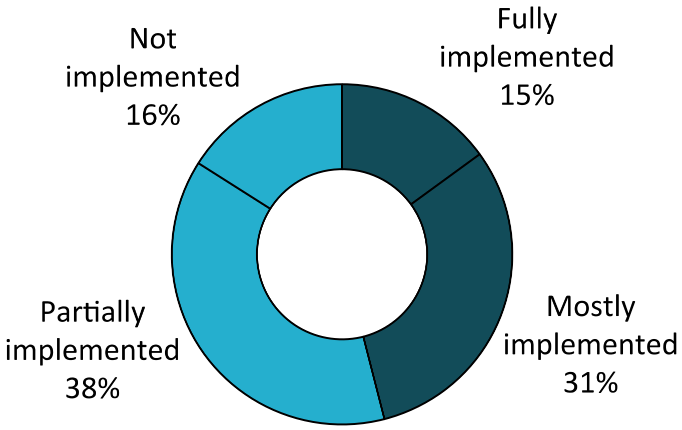
My organization effectively manages security risks to information assets, enterprise systems, SCADA networks and critical infrastructure



Security and compliance industry initiatives enhance the security posture of my organization



Compliance with security requirements is strictly enforced



Risks and investments are increasing, but confidence in the organization's ability to secure critical assets is not keeping up. How can this be? Based on ScottMadden's experience working with energy organizations, we can point to the following reasons:

- There is a lack of meaningful measures of cybersecurity progress
- Senior leadership is not engaged in cybersecurity decision making
- Cybersecurity efforts are not tied to enterprise risks
- Cybersecurity efforts are siloed and tend to be confined to what the IT and/or security organization can directly control

Successful organizations take a different approach to cybersecurity—they engage business stakeholders, focus organizational responses on enterprise risks, and deliver tangible outcomes. We call this strategic cybersecurity.

Strategic Cybersecurity Answers These Four Questions

1) What are the biggest cybersecurity risks to our enterprise?

- Risks are determined with senior leadership engagement—the security team does not do this by themselves
- Risks are used to establish priorities, focus management's time and attention, and create capital investments

2) What is the appropriate response to these risks?

- Desired cybersecurity capabilities are identified based on enterprise cyber risks and industry guidance

3) How will success be measured?

- Success is defined and appropriate indicators are used to monitor:
  - To what extent are our desired cybersecurity capabilities in place?
  - How well are our cybersecurity capabilities mitigating enterprise cyber risks?

4) How do we get there?

- A cybersecurity program is implemented to direct and monitor cybersecurity performance
  - A cybersecurity roadmap is created to achieve desired cybersecurity capabilities
  - Priorities are enterprise risk informed
  - Project management and organizational change management capabilities are provided to successfully implement
  - Monitoring of indicators drives corrective actions and continuous improvement

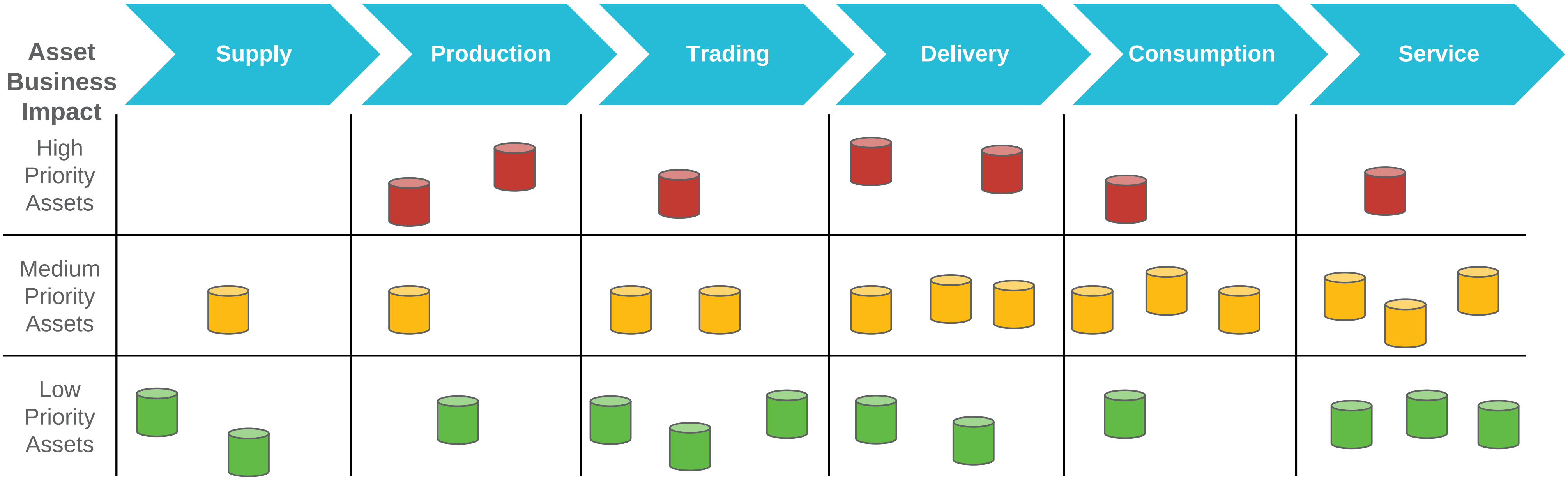
1) What are the biggest cybersecurity risks to our enterprise?

Determine Your Most Important Assets

All strategic efforts require an understanding of what is most important to achieving enterprise objectives. Strategic cybersecurity is no different. It focuses on what is most important rather than what is easiest to secure. Critical assets are not excluded because they are more difficult.

Understanding enterprise risks starts with determining "What am I trying to protect?"

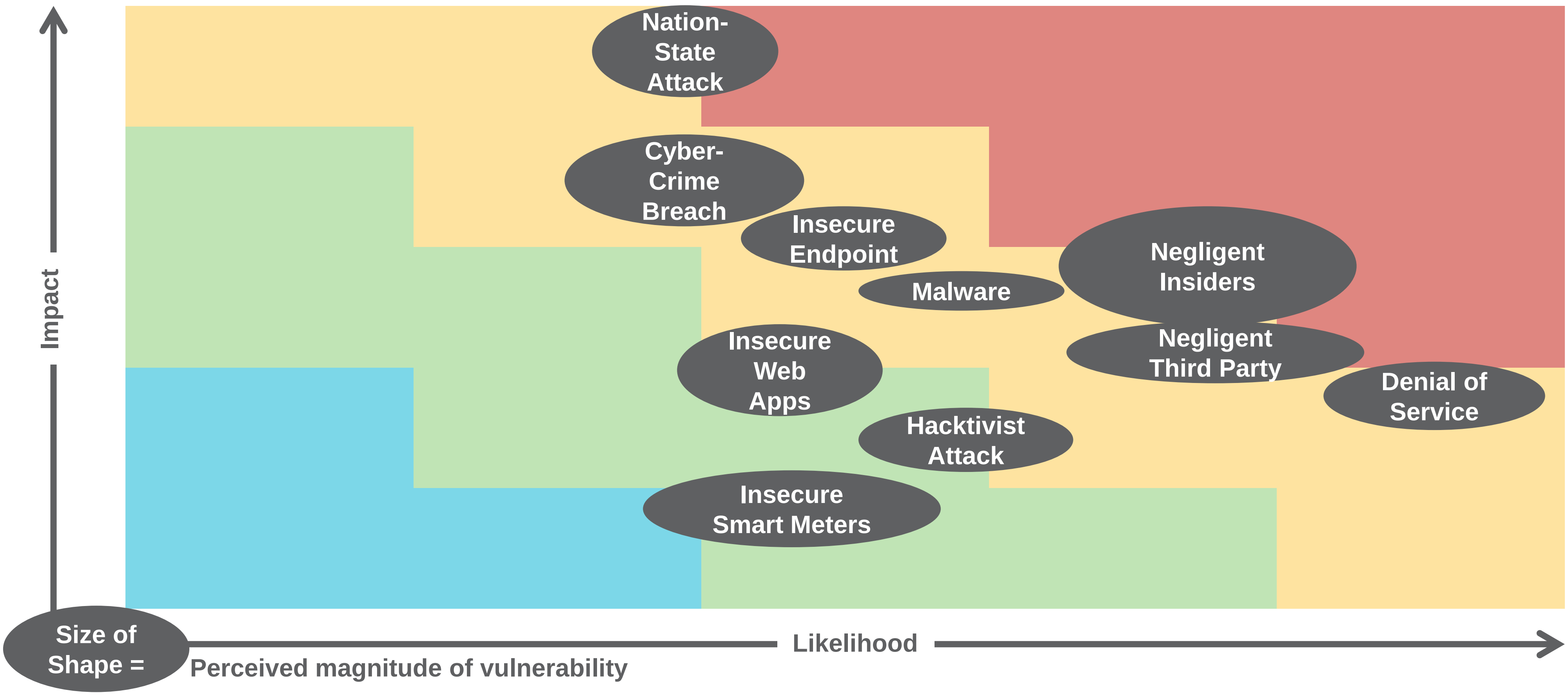
- Understand your mission critical business processes
- Identify which information assets support the success of these business processes and to what extent
- This is informed by, but not restricted to, compliance requirements
- This is inclusive of all enterprise technology assets—both OT and IT



Asset Business Impact	Supply	Production	Trading	Delivery	Consumption	Service
High Priority Assets		🟥🟥	🟥	🟥🟥	🟥	🟥
Medium Priority Assets	🟨	🟨	🟨🟨	🟨🟨🟨	🟨🟨🟨	🟨🟨🟨
Low Priority Assets	🟩🟩	🟩	🟩🟩🟩	🟩🟩	🟩	🟩🟩🟩

1) What are the biggest cybersecurity risks to our enterprise?

Engage Business Stakeholders in Enterprise Risk Discussion

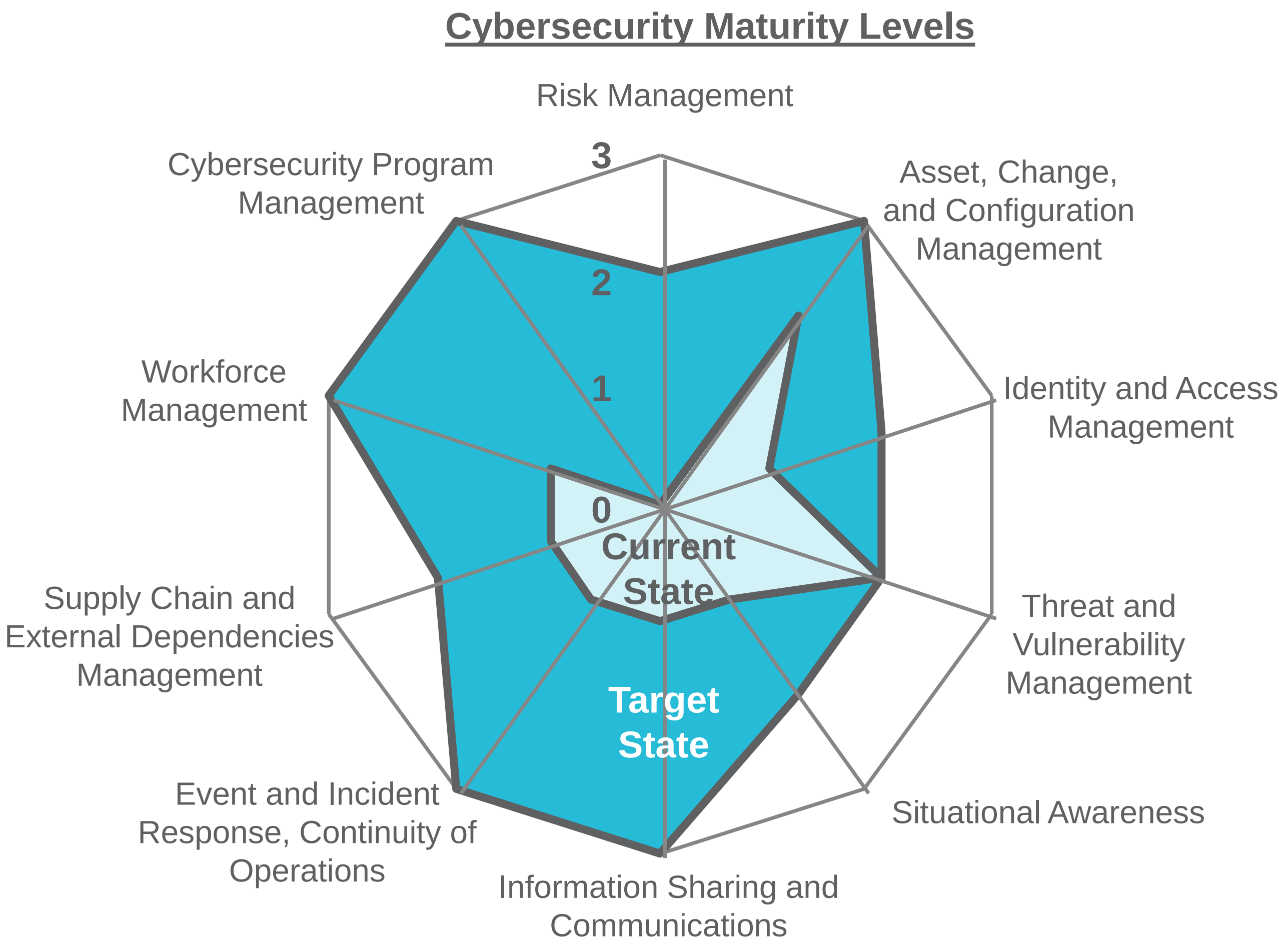


A business discussion of cyber threats makes them real. Your business community may not have deep knowledge of cyber risks, so discussions are mindful of the audience's knowledge level, but this does not let business leaders off the hook. They must have an acceptable understanding in order to provide thoughtful input into cybersecurity decision making and to sponsor cybersecurity efforts.

This does not need to be overly scientific—most companies do not possess precise measures of likelihood and impact. Instead, the discussion should serve to educate business leaders, to provide context for the cybersecurity program, and as a starting point that leads to a more detailed understanding of enterprise risks.

scottmadden
MANAGEMENT CONSULTANTS

Determine Desired Capabilities Based on Enterprise Risks



Cybersecurity needs to be managed as a business process. Cybersecurity is improved by maturing and continuously improving the capabilities that support this business process.

Start by using the Department of Energy's Cybersecurity Capability Maturity Model (C2M2) to determine cybersecurity capability gaps:

- Evaluate existing capabilities by technology asset owner (e.g., IT, generation, etc.)
  - Different owners will often have different maturity levels
- Evaluate desired maturity levels based on risk assessment results
  - Minimal (baseline) capabilities should be determined for all asset types using industry guidance
  - Target maturity levels should be informed by the criticality of the asset type
- Determine capability gaps and develop responses for high-priority gaps
  - Business leaders are engaged in both evaluating cyber risks and determining the appropriate response

Use Cybersecurity Metrics to Gain Confidence

Metrics are developed to eliminate uncertainty and build confidence in cybersecurity efforts. Use them to support decision making and demonstrate the value of cybersecurity. Metrics are developed using the following structured approach:

- Identify important cybersecurity risks
- Determine capabilities necessary to mitigate risks
- Develop questions that must be answered to assess progress toward implementing capabilities and mitigating cyber risks
- Create the metrics and collect the data that answer these questions

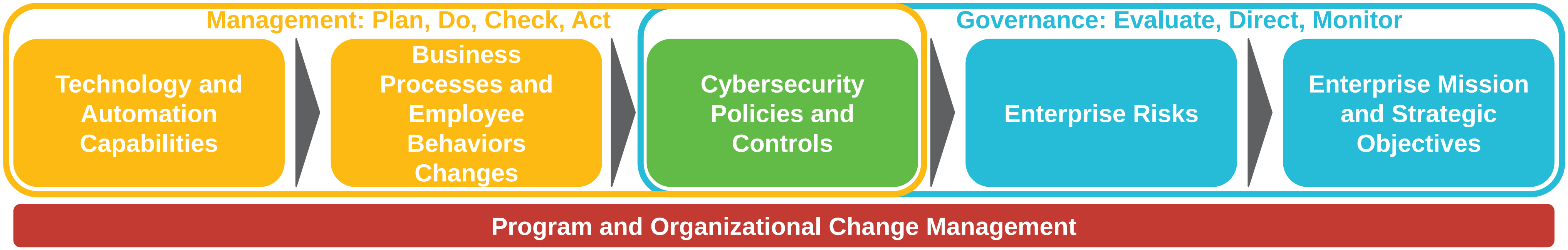
Risk	Mitigate exposure to unauthorized changes to critical infrastructure resulting from a cybersecurity attack or breach			
Mitigating Capabilities (C2M2)	Asset, change, and configuration management			
Questions	Have we implemented desired asset, change, and configuration management capabilities?	How much of the enterprise is under asset, change, and configuration management control?	How often are unauthorized changes made?	How well do we understand the cause of unauthorized changes?
Metrics	■ Current asset, change, and configuration management maturity level versus baseline maturity level ■ Current asset, change, and configuration management maturity level versus expected maturity level	■ Percentage of assets supported by conforming asset, change, and configuration management processes by business unit	■ Number of unauthorized changes identified in the last 12 months	■ % of unauthorized changes due to lack of process conformance ■ % of unauthorized changes due to known malicious behavior ■ % of unauthorized changes unexplained

A Programmatic Approach Delivers Strategic Outcomes

Organizations attempt to build and improve cybersecurity capabilities through a series of individual projects. The problem is that this leads to siloed or disjointed efforts. This comes from thinking in terms of discrete parts rather than a cohesive whole:

- Projects are initiated to address tactical needs by focusing on individual capabilities
- As other necessary capabilities are identified, new independent projects are launched
- Unfortunately, this approach often leads to an outcome that can be less than the sum of its parts

A programmatic approach delivers strategic outcomes by coordinating individual efforts that address the entire system.

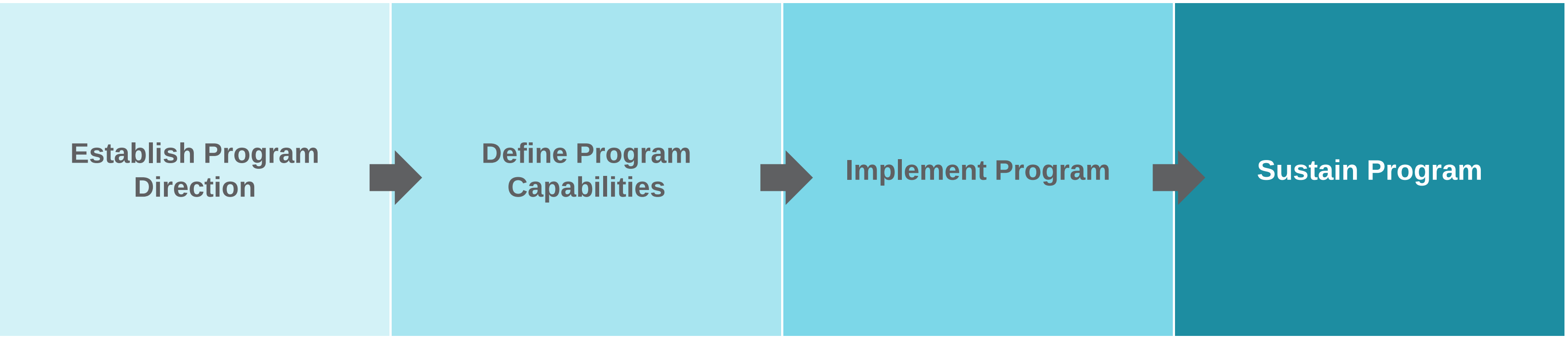

Management: Plan, Do, Check, Act
Governance: Evaluate, Direct, Monitor
Technology and Automation Capabilities
Business Processes and Employee Behaviors Changes
Cybersecurity Policies and Controls
Enterprise Risks
Enterprise Mission and Strategic Objectives
Program and Organizational Change Management

The cybersecurity program includes the following:

- Program Governance and Oversight
  - Sets program direction, monitors performance against direction, and establishes management accountability for program objectives within the context of cybersecurity policy
- Policy Framework
  - Aligns enterprise cybersecurity policies and controls with program objectives and energy industry guidance
  - Establishes the enterprise cybersecurity expectations
- Cybersecurity Functional Management
  - Responds to program direction and facilitates achievement of cybersecurity program expectations throughout the enterprise
- Program Implementation Capability
  - Coordinates and aligns cybersecurity project efforts and supports organizational change management in order to achieve desired outcome—mitigation of enterprise cyber risk to enterprise mission and strategic objectives

Putting It All Together

Building and Sustaining a Cybersecurity Program



Establish Program Direction

- Develop program charter
  - Determine guiding principles
  - Define scope
  - Design governance
  - Design policy framework
- Evaluate enterprise risks

Define Program Capabilities

- Assess current capabilities
  - C2M2 assessment
- Define target state
- Identify and prioritize gaps based on:
  - Risks
  - Gap size
  - Capability dependencies

Implement Program

- Determine required business changes
- Determine organizational roles and responsibilities
- Determine resource and skill requirements
- Create roadmap by:
  - Control
  - Asset
  - Business unit
- Launch and manage program

Sustain Program

- Implement functional and control ownership
- Define and implement measures
- Implement assurance and continuous improvement processes

Engaging senior leadership in cybersecurity decision making is the single most important factor in creating a successful cybersecurity program—more than technology or funding.

ScottMadden's Cybersecurity Services

Cybersecurity Program Services

- Design and implementation
- Assessment
- Transformation

Cybersecurity Governance Design and Implementation

- Policy framework design
- Policy alignment (including alignment with NIST Cybersecurity Framework)
- Cybersecurity metric design and implementation

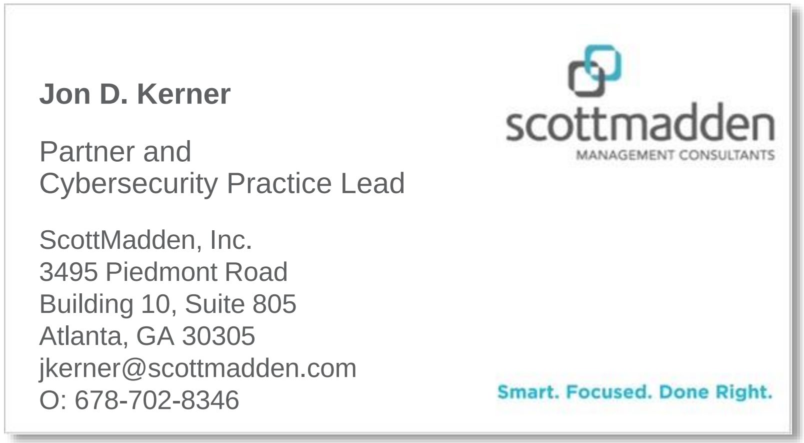
Cybersecurity Organizational Change Management (OCM)

- OCM support of implementation efforts
- Cybersecurity awareness plan—design and implementation

Cybersecurity Capability Design and Implementation

- Process design
- Vendor selection
- Implementation project management

To Learn More About Strategic Cybersecurity, Contact Us



Jon D. Kerner

Partner and
Cybersecurity Practice Lead

ScottMadden, Inc.
3495 Piedmont Road
Building 10, Suite 805
Atlanta, GA 30305
jkerner@scottmadden.com
O: 678-702-8346

scottmadden
MANAGEMENT CONSULTANTS

Smart. Focused. Done Right.