scottmadden
MANAGEMENT CONSULTANTS

Smart. Focused. Done Right.®

Cybersecurity Operating Model

Webinar

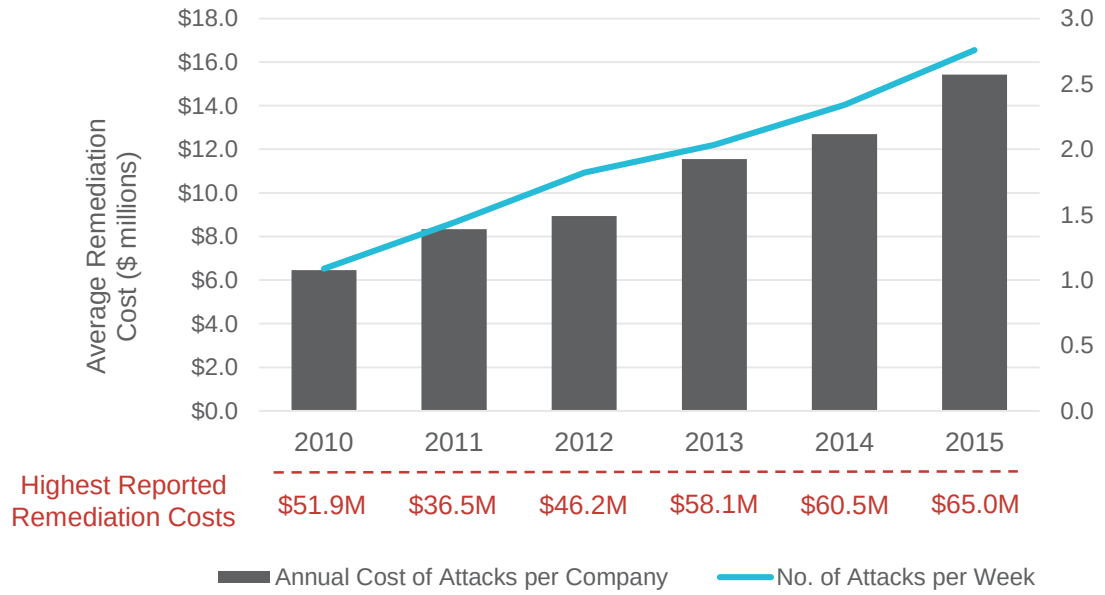
June 2018

Cyber Attack Trends Continue to Increase in Complexity, Frequency, and Severity

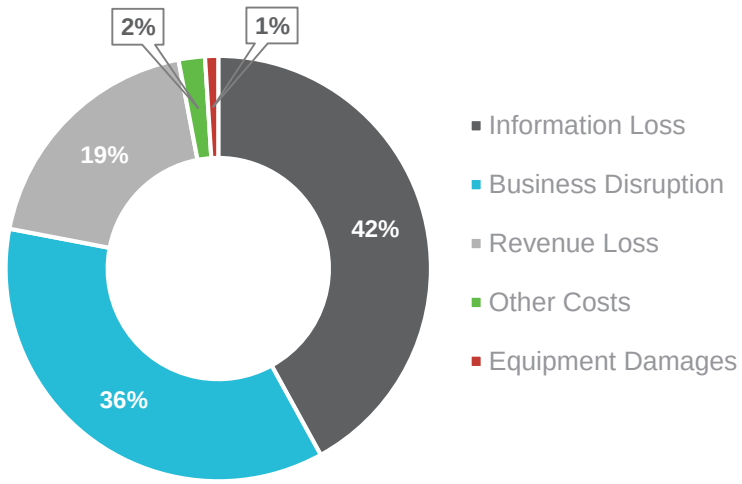
Significant data breaches included[1]:

- VTech (children's technology maker) – personal data compromised for 5 million parents and 6 million children
- Kaspersky Lab (security vendor) – 13 million account records exposed
- Experian (credit service provider) – personal data compromised for 15 million customers
- U.S. Office of Personnel Management (federal government) – PII and restricted data exposed for 21.5 million federal employees
- Anthem Blue Cross Blue Shield (health insurer) – PII and restricted data exposed for 80 million patients and employees

Cyber Attack Trends[2]



Cyber Attack Cost Breakdown[2]



The average organization spent more than $15 million remediating the effects of cyber attacks. To mitigate potential costs, organizations must take action to understand and protect the flow of their sensitive information.

1. CRN, 10 Biggest Data Breaches
2. Source: Cost of Cyber Crime Study, Ponemon Institute

scottmadden
MANAGEMENT CONSULTANTS

Security Organizations Are Very Busy, but Can They Answer the Question "Are We Becoming More Secure?"

Reactive

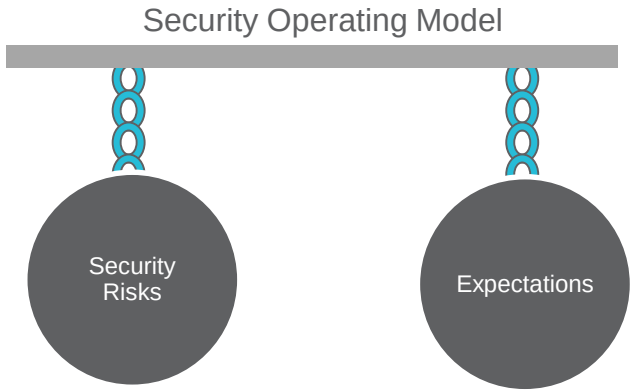
In many organizations, security efforts are focused on deploying technologies, implementing "best practices," or responding to a continuous stream of alerts and issues. The result is a reactive security organization, busy with activity and unable to answer the question "are we becoming more secure?"

- The result is friction and distrust between business leaders and the security organization
- Security efforts are seen as expensive—doing more to slow rather than secure the business

Strategic

A more strategic approach is necessary. It acknowledges the reality that security needs will always exceed security capacity, provides direction to optimize security resource allocations, and demonstrates progress toward a more secure organization. This approach requires fundamental changes in security:

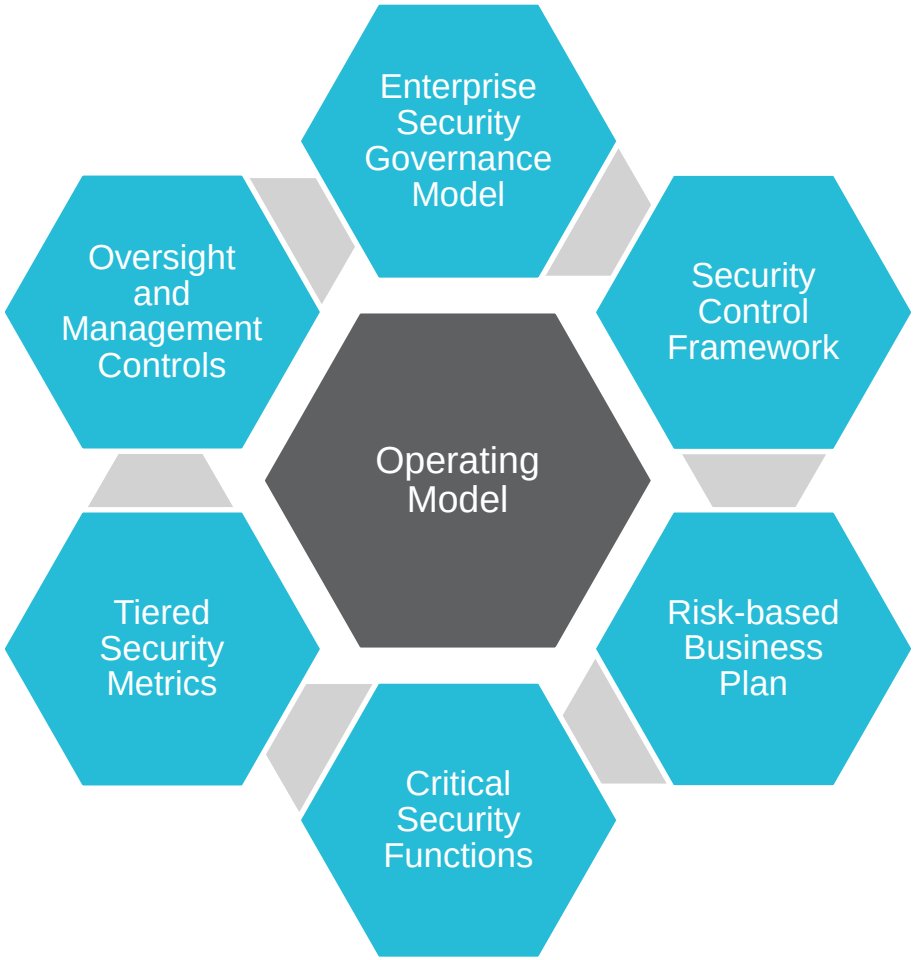
- Shift focus from implementing security controls to identifying and managing security risks
- Expand collaboration with the business to ensure transparency of security metrics
- Implement a holistic security operating model to balance risks with expectations



scottmadden
MANAGEMENT CONSULTANTS

Security Operating Model Is Designed to Continuously and Transparently Improve Security across the Organization

Understanding that everything cannot be secured, a security operating model utilizes a risk-based approach to identify and prioritize risk mitigation efforts to appropriately secure the enterprise's mission.



Enterprise Security Governance Model
Establishing a security executive committee with senior leadership from across the organization can balance the security risks to the organization with the overall costs.

Security Control Framework
An industry-accepted controls framework provides the structure and guidance to identify best practices and target gaps in potential security coverage.

Risk-based Business Plan
The objective of the business plan is to allocate security resources appropriately based on the risks to the organization.

Critical Security Functions
Core functions represent areas so vital for success there must be formally controlled guidance and expectations through policies, programs, processes, and tools.

Tiered Security Metrics
"What gets measured gets improved." Security metrics are critical to understanding the health of the core function and provide a transparent picture of the security of the organization.

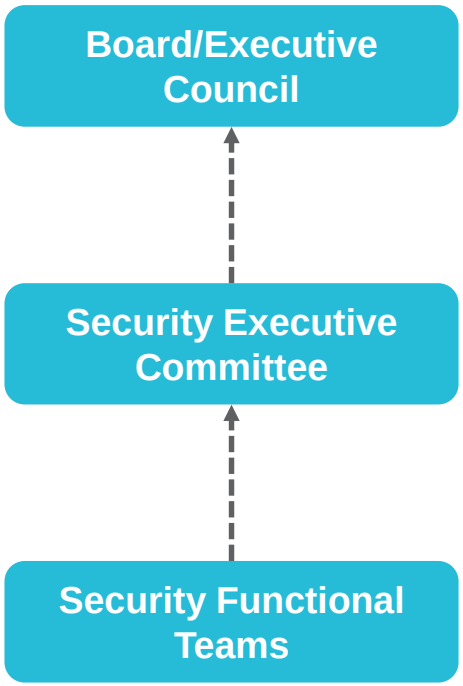
Oversight and Management Controls
Management oversight ensures everything ties together like a continuous improvement loop. Management controls ensure the organization is readily able to check performance and adjust direction as needed.

scottmadden
MANAGEMENT CONSULTANTS

Enterprise Security Governance Model Enables and Ensures Collaboration with the Business

Establishing a security executive committee with senior leadership from across the organization can balance the security risks to the organization with the overall costs

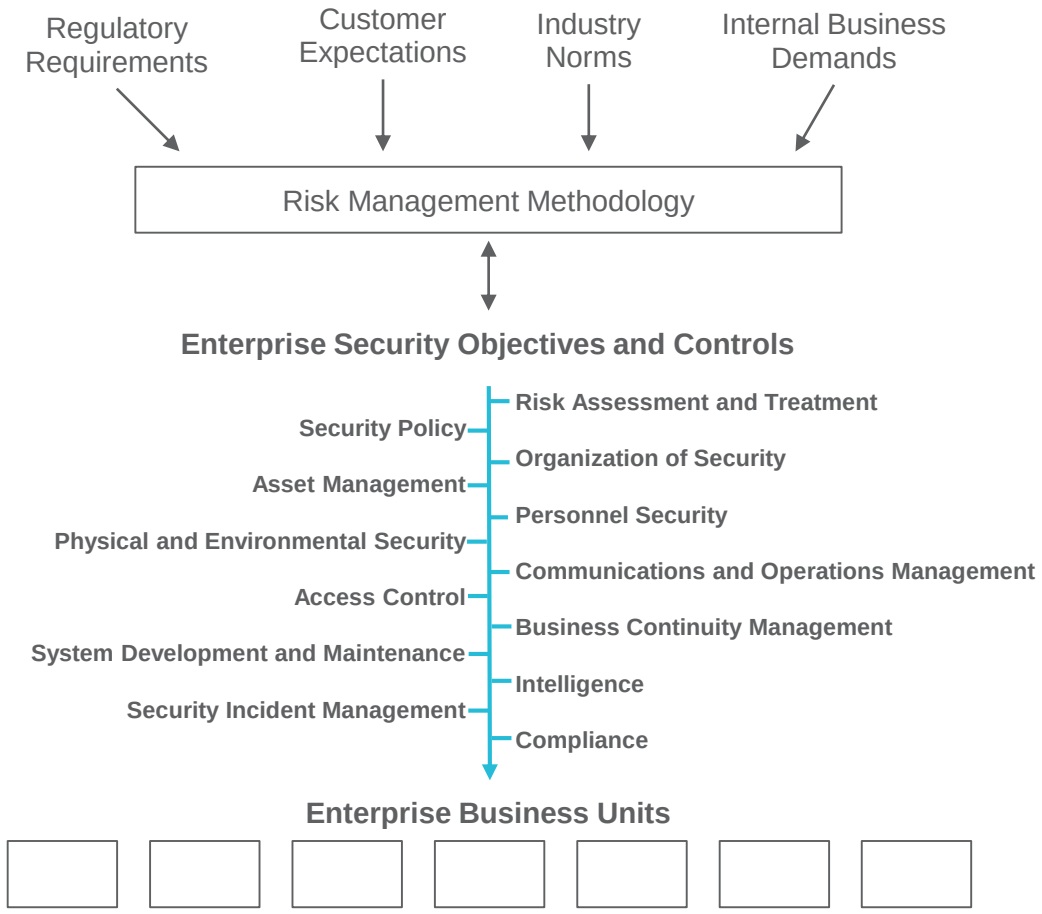
- Securing a complex enterprise can be very daunting. Without proper enterprise governance, the security costs can escalate rapidly
- The purpose of the steering committee should evolve with the maturity of the operating model and the evolution of the risks facing the organization
  - Initially, this group will assist with defining scope and target capabilities
  - After establishing core capabilities, the role should shift to more of an oversight body responsible for championing enhancements
- This prioritization and decision making cannot be performed in a silo as the boundaries of each asset type are easily debatable
- Partnership and alignment among organization leads is critical to successfully defining and refining a clear scope as risks evolve and capabilities mature



Transparency and balancing risk management decisions are critical to governing a holistic security operating model.

Security Controls Framework Establishes the Backbone of Enterprise Security

Utilizing an industry-accepted framework ensures alignment with industry expectations and provides a method for regular capability assessment to track and measure progress.



Benefits

- Provides the structure and guidance to identify best practices and target gaps in potential security coverage
- Quantifies and codifies desired security behaviors into a universal language
- Provides a way to consistently educate and communicate with stakeholders in a language everyone can understand
- Provides universal communication tools to external customers for compliance and benchmarking

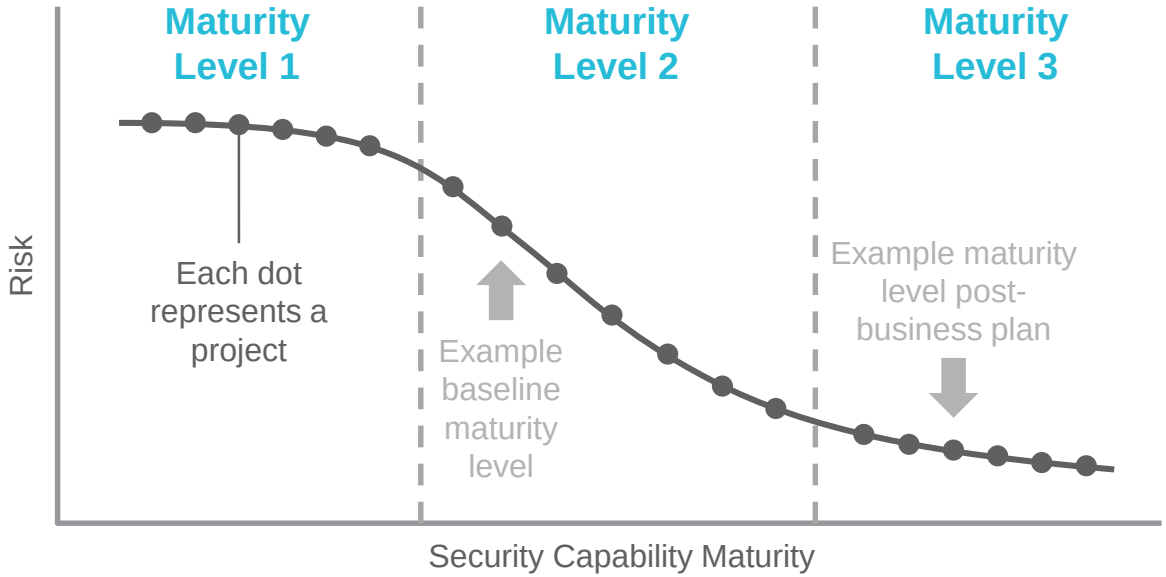
scottmadden
MANAGEMENT CONSULTANTS

Business Plan Allocates Resources Based on Risk

The business plan is the most powerful tool to ensure alignment across the entire operating model based on risk to the organization.

The business plan includes four critical building blocks:

- **Security risk assessment and treatment plan**: allows an organization to understand the residual security risk the organization is accepting based on the implementation of a security controls framework, core function performance, and control compliance metrics
- **Capability maturity**: utilizing a consistent and industry-based maturity model assessment can help identify the maturity level of security capabilities and define target achievement levels. The results of these assessments can also be utilized to benchmark capabilities with similar organizations
- **Performance gaps**: by utilizing performance metrics, the security organization and their stakeholders will have a good understanding of their control performance and desired targets to support individual strategic objectives
- **Control and scope evolution**: based on the risk to the organization, security may look to improve functionality or efficiency of existing controls. Additionally, the scope of the controls could evolve to apply to a larger subset of assets



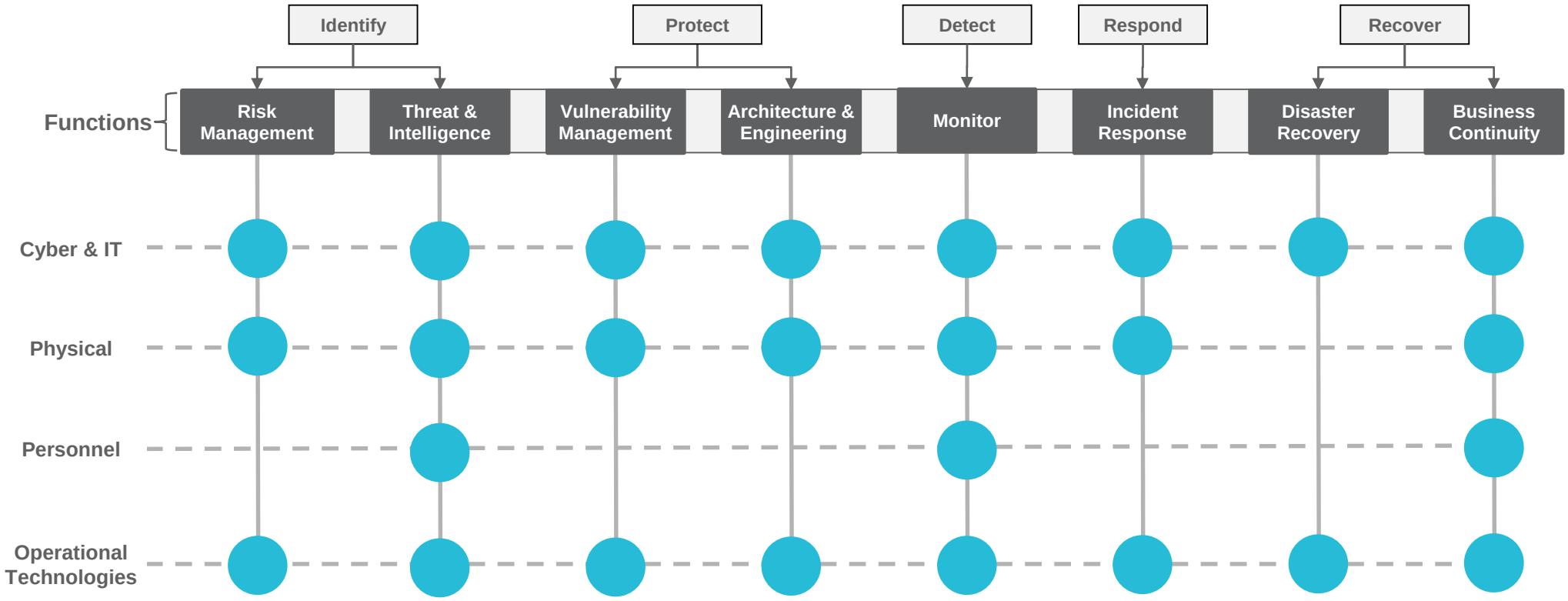
- Each project implements similar security capabilities within maturity level
- Lower maturity capabilities must be implemented before higher maturity capabilities
- Projects are sequenced by risk impact

The desired end state is a security program that aligns with the industry-accepted controls framework and your chosen level of maturity.

scottmadden
MANAGEMENT CONSULTANTS

Security Functions Establish Clear Lines of Ownership

Organizations typically face challenges defining the appropriate levels of accountability as they grow in size, scope, and complexity. Typically, we see security organizations structured around asset types which causes duplicity of effort as well as gaps in the holistic enterprise coverage.

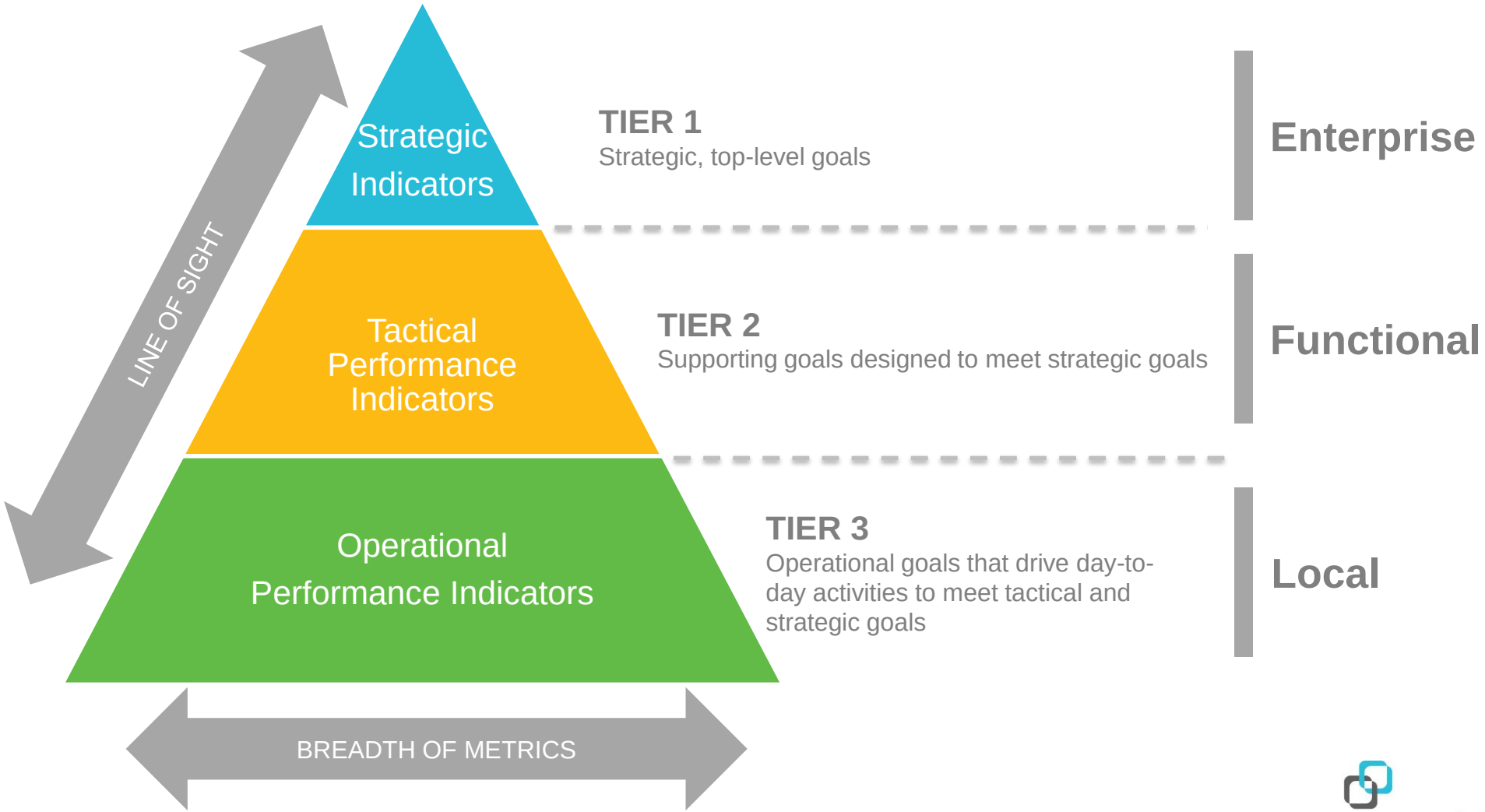


Functional organization provides parametric decision support to share best practices across asset types, provides clear boundaries of accountability, and ensures holistic security coverage.

scottmadden
MANAGEMENT CONSULTANTS

Tiered Security Metrics – What Gets Measured Gets Improved

Security metrics are critical to understanding the health of the core function and provide a transparent picture of the organization's security.



scottmadden
MANAGEMENT CONSULTANTS

Oversight and Management Controls Ensure Performance Meets Expectations

The results of the management and controls oversight provide transparency on the adoption of the controls framework, inform the governance structure, challenge the scope, and lead to gap-based and risk-informed initiatives for inclusion in the business plan.

Key components:

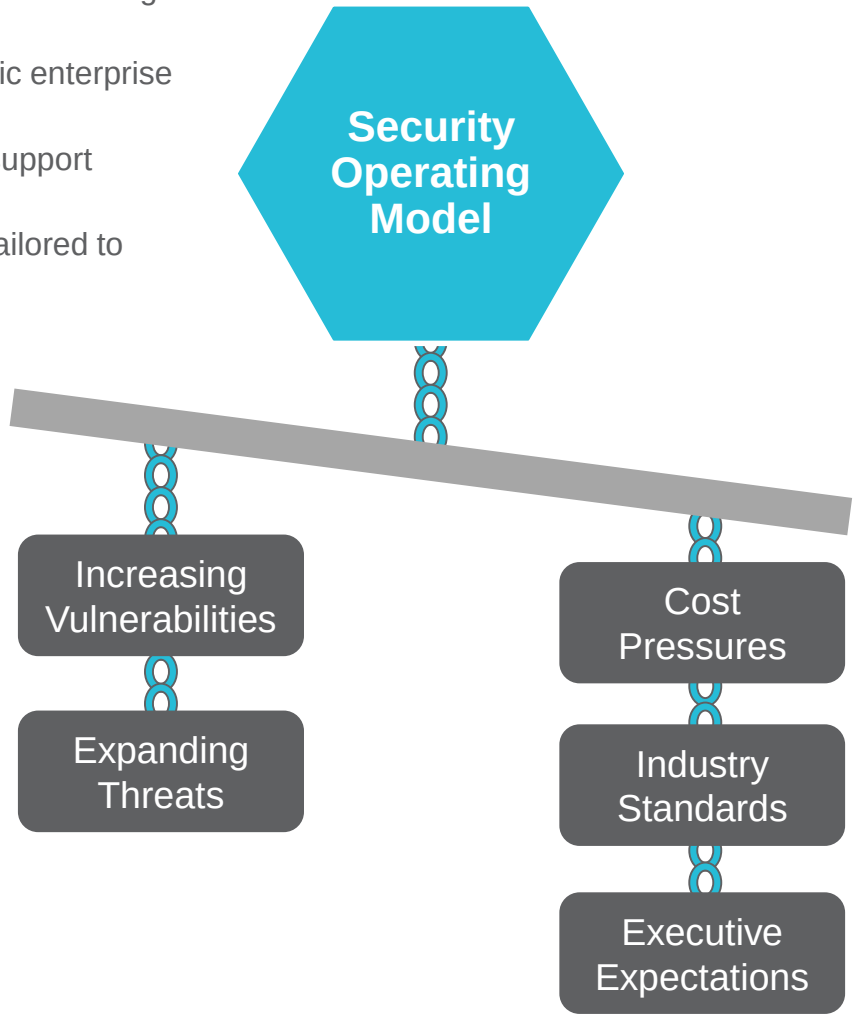
- **Performance Metrics/Outcomes** – Developing, implementing, and monitoring a comprehensive set of core function performance metrics in order to set expectations and identify gaps or adverse trends
- **Self-assessments** – Self-assessments answer the question "how are we doing?" Self-assessments evaluate core function performance in a given area by determining current performance, identifying gaps between current and desired performance, and defining strengths and deficiencies. A self-assessment plan is developed and reviewed at the beginning of each year
- **Management Review Meetings** – MRMs ensure leadership is effectively informed and engaged in driving the performance of their respective areas. An MRM is a regularly scheduled meeting to ensure management oversight of organizational performance, identify learning opportunities, and support continuous improvement
- **Corrective Action Program** – CAP is a standard approach for issue resolution that provides a formal list of risk-based prioritized issues, consistent process to investigate and resolve issues, and mechanism to track all corrective actions
- **Peer Groups** – Peer groups communicate frequently and meet regularly to collectively analyze/monitor core function performance metrics, identify gaps, and drive continuous improvement and core function oversight and support

Management controls ensure the organization is readily able to check performance and adjust direction as needed.

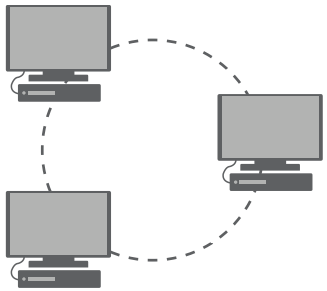
Conclusion

A security operating model balances risks to the organization within industry expectations and drives decisions about where to invest security resources

- Scope, vision, and mission should be grounded in securing high-risk areas using levels of layered security
- Core functions should focus on the cross-asset capabilities and holistic enterprise coverage
- Metrics should be tiered to provide varying levels of information and support organizational transparency
- Controls framework should be based on industry best practices and tailored to the organization's risk tolerance
- Business planning process should begin with an understanding of the high risks to the organization and focus the resources needed to implement foundational capabilities and remediate high risks
- Management and oversight activities should ensure proper focus and transparency to allow for adjustments

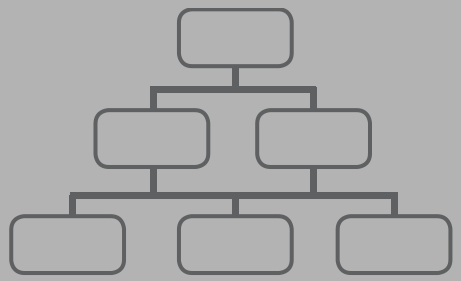


How ScottMadden Can Help



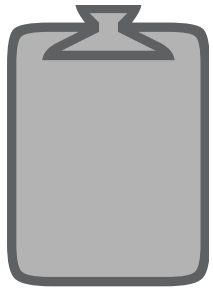
Cybersecurity Program Services

- Strategic planning support
- Security program management
- Design and implementation
- Security policy alignment
- Program assessments
- Sensitive data inventories
- Transformation



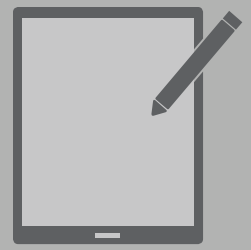
Cybersecurity Governance Design and Implementation

- Policy framework design
- Business policy and process assessments
- Data security standards creation
- Cybersecurity metric design and implementation
- Access management strategy development



Cybersecurity Organizational Change Management (OCM)

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



Cybersecurity Capability Design and Implementation

- Process design
- Implementation project management
- Cybersecurity threat-based risk assessments
- Vendor selection

scottmadden
MANAGEMENT CONSULTANTS