Committee(s)	**Dated:**
Digital Services Sub Committee (DSSC)	1st November 2019
Subject: The case for a Security Operating Model	
Report of: Chamberlain	**Public** **For Information**
Report author: Gary Brailsford-Hart ,Director of Information & Chief Information Security Officer	

Summary

The City of London is dependent on IT to facilitate business operations. In today's knowledge-driven economy, information is critical to the City of London's ability not only to survive, but also to thrive. Experienced business leaders know that information deserves at least the same level of protection as any other asset, and have included information security as an addition to the senior board.

However, information security faces a myriad of challenges, including changing risk profiles, lack of funding, cultural issues, and internal and external threats. Managing information security has never been so critical, yet there are very few formal models that help information security do so effectively. Of the few models that do exist, even fewer consider how the enterprise changes, how the culture adapts, and what may or may not emerge as a result. Current models tend to be static and simple, while environments are continuously changing. The City of London requires a Security Operating Model that recognises that it is a dynamic organisation, and provides a way the information security function can take a holistic approach to managing information security while directly addressing business objectives. The model must also provide a common language for information security and business management to talk about information protection.

Recommendation(s)

Members are asked to:

- Support the development of a Security Operating Model;
- Endorse the identified measures within the 10 steps gap analysis.

Main Report

Background

1. Monitoring the state of security across the last twelve months within the City of London has identified a clear focus almost exclusively on deploying technologies, implementing "best practices," or responding to a continuous stream of alerts and issues. The result has produced a reactive security function, busy with activity but unable to address the more pressing needs of preparedness and getting ahead of the alert. This has sometimes resulted in challenges between the business and the delivery needs of the security function. Security efforts are seen as expensive—doing more to slow rather than secure and enable the business.

2. A more strategic approach is necessary. It acknowledges the reality that security needs will always exceed security capacity, provides direction to optimise security resource allocations, and demonstrates progress toward a more secure organisation. This approach requires the security function to transition from security performance to strategic security by:

   - Changing the focus from security controls to security risks: Risk is the basis for all security decision making and performance management;
   - Transitioning ownership of security risks: The security function does not own security risk decisions, the business does;
   - Implementing a security operating model to govern this strategic approach: Establishing priorities, expectations, and oversight of risks and efforts to address them.

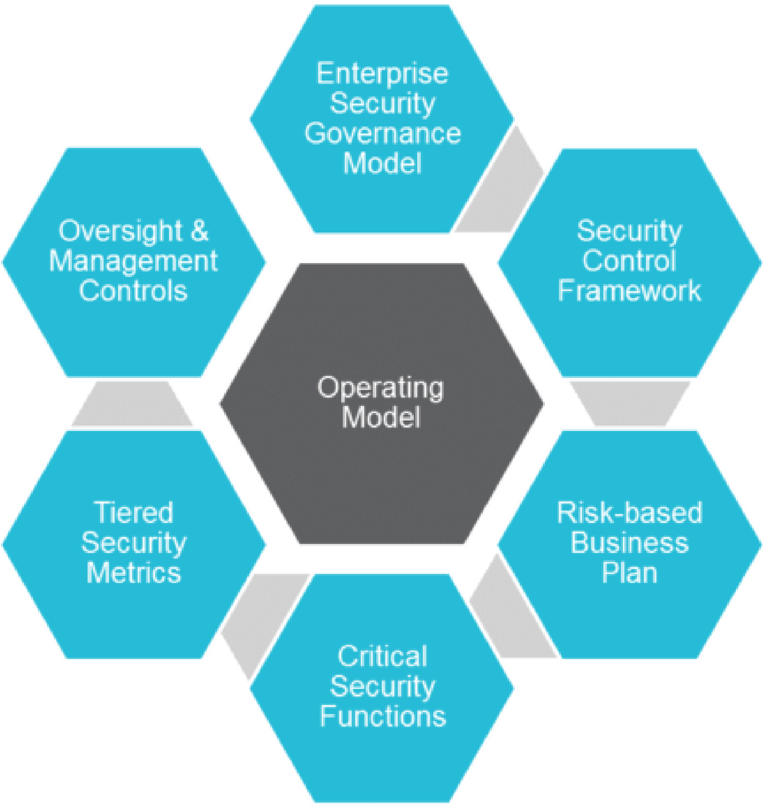
3. The security functions focus is on identifying risks, recommending responses to these risks, facilitating the appropriate tradeoff decisions related to these risks, and providing line of sight to the execution of these risk responses.

4. A security operating model enables this approach. It provides governance and oversight of security across the City of London, where the business is not only a recipient of the security services, but is also instrumental in the collaboration,

implementation, and sustainability of security efforts. When viewed holistically, the operating model utilizes a risk-based approach to identify and prioritize risk mitigation efforts to appropriately secure the enterprise’s mission. The core of a security operating model is a collaborative continuous improvement process designed to sustain the controls that secure the enterprise.

Implementing a Security Operating Model

5. There are 6 Components of the Security Operating Model these are described in the narrative below:


Enterprise Security Governance Model
Security Control Framework
Risk-based Business Plan
Critical Security Functions
Tiered Security Metrics
Oversight & Management Controls
Operating Model

- **Enterprise Security Governance Model**
  Establishing a security executive committee with senior leadership from across the organisation can balance the security risks to the organisation 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 organisation.
- **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 organisation.
- **Oversight & Management Controls**
  Management oversight ensures everything ties together like a continuous improvement loop. Management controls ensure the organisation is readily able to check performance and adjust direction as needed.

6. The security operating model can be delivered through:

- Clearly defined governance and oversight responsibilities, including scope of asset responsibilities
- A risk-based planning process that engages business stakeholders in risk tradeoff decisions and prioritizes security investments and utilization of scarce resources
- A security program that defines and documents security expectations of asset owners throughout the enterprise
- Oversight mechanisms that provide an objective view of enterprise security risks and performance against the security controls, both implementation and sustaining performance

7. This model provides the City of London's agreed-upon approach for responding to security risks and establishes expectations for who is responsible for what. This becomes the baseline that security performance is monitored against.

Ten Steps Gap Analysis

8. A ten steps gap analysis has been undertaken against the SANS 20 Critical Security Controls and is provided at Appendix 1. This analysis identifies a requirement for continued investment in additional controls across staffing, services or product purchasing. Where security improvements are identified these should be considered in the total security context across the CoL environment and, where appropriate, seek to reduce costs through a joint solutions approach that benefit not only the core network services but also institutional departments.

Conclusion

9. The gap analysis undertaken against the current control framework identifies a number of areas requiring enhancement and attracting expenditure. The development of a Security Operating Model across a three year plan would provide the City of London the ability to smooth future expenditure, provide a robust framework for risk management and mitigation, and enhance the resilience capabilities into current and future programmes.

Appendices

- Appendix 1 – NON-PUBLIC: Security Operating Model Gap Analysis

Gary Brailsford-Hart

Director of information & Chief Information Security Officer

T: 020 7601 2352   E: gary.brailsford@cityoflondon.police.uk