A Disciplined Approach to CYBERSECURITY PROGRAM MANAGEMENT

Brian Hubbard
Director of Commercial Strategic Business and Cybersecurity Solutions
Edwards Performance Solutions

In many organizations, the Chief Information Security Officer (CISO) and their team understands the need for a strategic approach to managing an enterprise information security program. However, continual tactical "fire drills" rarely allow time to be dedicated to strategic objectives.

Given typical CISO resource constraints, efficient and effective operations is critical to success. Running a cybersecurity program through a disciplined program management approach enables CISOs to bridge gaps between tactical time pulls and the goals of a strategically oriented, business focused information security program. For smaller organizations that may not have a security staff at all, the Cybersecurity Program Management Office (PMO) concept provides a model for obtaining the necessary services.

ESTABLISHING A CYBERSECURITY PROGRAM

To escape day-to-day fire drills, a business must establish a framework for its cybersecurity program, such as the widely adopted NIST Cybersecurity Framework (CSF). The CSF focuses cybersecurity decision making as a function of business risk and defines the major functions of a cybersecurity program as Identify, Protect, Detect, Respond and Recover. It further provides a set of control for activities with desired outcomes within each function. The Identify function specifies business priorities. Before making security investments, a business must understand what its information and system assets are, what their criticality to the business is, what their vulnerabilities are and what risks they can pose. An understanding of risk posture and risk management strategies include risks created by suppliers.

Once business assets and risks are understood, appropriate protective measures that mitigate business risks inherent to the operational environment are identified. Protective measures include activities such as:

- Limiting access to authorized users, processes, or devices and to authorized activities and transactions.
- Establishing security policies, processes, and procedures/guidelines.
- Training employees on cybersecurity procedures and policies.
- Ensuring information is managed consistently with the company's risk strategy.

Even with the best protective mechanisms in place, a business's cybersecurity risk will not be completely

mitigated. Routine monitoring is necessary to quickly detect malicious, undesirable, or abnormal activity. It is less costly to be proactive than to wait until law enforcement, a client, or the press provides notification of a breach.

Breaches will happen. Once a breach has been detected or identified, a rapid, rehearsed response is necessary. The plan must be exercised and maintained in "peace time" to ensure its effective execution in the event of an actual crisis. A communication strategy is needed to communicate breach and response plans (before the event) and information (during the event) to both internal and external stakeholders. This ensures that all stakeholders understand what to expect and how to react to a breach.

Successful recovery requires planning to save time, money, information, and to prevent reputational damage. Businesses must plan to recover client trust, and to expend the resources necessary to recover from a breach. Cyber liability insurance is one mechanism that can be used to mitigate the costs associated with a breach. Having a solid plan in place minimizes the long-term impact of a breach on the business.

MANAGING THE CYBERSECURITY PROGRAM

Making a cybersecurity program successful requires a continuous, disciplined management approach. Managing the cybersecurity program through a PMO structure establishes the information flows and management routines that will allow the CISO to move into a more strategic role and focus on continuous improvement instead of continuously operating in crisis mode. "Fires" will still happen, but they will not interfere with the smooth operation of the overall program. For organizations that don't have a dedicated cybersecurity staff, outsourcing can be an effective tool for optimizing their resources.

COMPONENTS OF THE CYBERSECURITY PMO

A cybersecurity PMO comprises six major components: Risk Management, Compliance, Policy and Procedure Management, Vulnerability Management, Security Project Management, and Knowledge Management.

Risk Management

Risk management is the ongoing process of balancing business opportunity with the impact of threats exploiting vulnerabilities. The Risk Management function is the engine that drives the program. The Risk Management function leverages industry best practices and standards as well as best of breed tools to determine the value at risk for the business and thus the level of resourcing appropriate for mitigation efforts. The risk register and risk assessments are continuously updated, monitored, and tracked with input from the other components.

Compliance Management

Compliance, whether with internal standards and policies or regulatory requirements, can be a major issue for any information security program. It is also a risk that must be managed, and can consume a large percentage of information security resources. Compliance should be a natural outcome of a well-structured cybersecurity program. The cybersecurity PMO streamlines these compliance issues by managing compliance through the CSF. Compliance is continuously monitored and tracked. Should an external audit be required, the Compliance Management function will support auditors inquiries, and serve as an Audit Liaison for the business.

Policy Management

Every business needs well-defined policies and procedures that reflect risk management decisions. Policies can only be enforced if they are up-to-date, relevant to the business, and communicated appropriately. The Policy Management function develops, updates,

communicates and stores the policies and procedures for the business.

Vulnerability Management

Information security is not an operation to be implemented once and forgotten. It is continually maintained and matured as the business grows. The threats to the organization and the vulnerabilities that could compromise its most vital assets are constantly changing. Many organizations conduct a vulnerability scan once or twice a year. The vulnerability management function comprises services that continuously assess system vulnerabilities. This could be a passive vulnerability scan or a more active "red team" service that closely matches the operational cadence of real-world attacks. As vulnerabilities or issues are uncovered, the responses are prioritized through the Risk Management function and new projects and/or tasks are created and tracked to completion.

Knowledge Management

The Knowledge Management function collects and maintains information that is relevant to the information security program. This includes detailed information about the information security program as well as tools and templates used to implement the program. The function also provides dashboards enabling leaders to easily understand the status of the security program at any time. The dashboards provide the CISO instant and up-to-date insight into the metrics in which their stakeholders are interested. Providing dashboards communicating CSF outcomes also provides a common language from the board level down to operations.

Security Project Management

An information security program is never static. There will always be areas for improvement, new vulnerabilities to correct, policies to update, assessments to conduct, new technology to incorporate, etc. The Security Project Management component leverages the best practices in the areas of operational performance and project management to organize and manage the projects required to make the information security program function. This function develops the organization's project roadmaps to fill gaps, develops plans of action, develops and socializes business cases for projects, and performs project budgeting, monitoring and control. This component also supports resource management through an integrated master plan and schedule.

CONCLUSION

Regardless of size, every organization needs to have a cybersecurity program that is focused on business success. Structuring around the NIST CSF and using the cybersecurity PMO organizational construct, every business can move cybersecurity from an unknown business risk to a business asset. To get started, take stock of what assets are important to the business and understand the risk to those assets. If the security team is overwhelmed with day-to-day issues, and the only board reporting is on how the problems of the month have been resolved, use the cybersecurity PMO to help restructure and manage the program. Don't wait until after a major breach to begin thinking about the structure of your program. For large businesses, doing nothing could be very costly to the business in lost profits, lost productivity, and lost reputation. For small businesses, not having a professionally managed cybersecurity program in place could be catastrophic.

About the Author

Brian Hubbard *is the Director of Edwards' Commercial Strategic Business Unit (SBU) and Cybersecurity Solution Area. Brian is responsible for all strategic Commercial and cybersecurity based initiatives. Brian is a strategic business leader with three decades of experience architecting, designing, and developing solutions to address some of the nation's top cybersecurity challenges. Brian was also a primary author and led the contractor team supporting NIST in the development of the Cybersecurity Framework.*

EDWARDS PERFORMANCE SOLUTIONS