ENTERPRISE CYBERSECURITY MANAGEMENT

Technology Whitepaper

ABSTRACT

The ability to understand the effectiveness and communicate security posture effectively is one of the most challenging issues that CISO's face today. This capability is critical when securing resources, aligning security with organization's risk profile, and in being able to show due care on behalf of the organization in the event of a compromise. SmarterD's Enterprise Security Management Platform addresses this critical gap in enterprise cybersecurity management through an innovative approach by continuously linking your cybersecurity capabilities to operational threat, vulnerabilities, business and IT capabilities, financial and market data directly to strategic cybersecurity planning decisions.

VIJAY SUNDHAR

Overview

The past twenty years in cybersecurity have been an incredible study in the hyper-growth and evolution of an industry. During this period, technology has evolved from non-stateful network layer firewalls as primary control, to today's container-based application layer controls and everything in between. Operationally, we have gone from health and availability monitoring to User Behavior Analytics and predictive control methods using enterprise SIEM technology. Incident response has effectively evolved into its own sub-industry with focus on forensics, threat hunting, and response reediness.

Despite these advancements, hyper-growth has left equally important areas of cybersecurity struggling to keep up. Even the most tenured CISOs are being challenged by the increasing demands or the role and needs of their stakeholders. The ability to understand the effectiveness and communicate security posture effectively is one of the most challenging issues that CISO's face today. This capability is critical when securing resources, aligning security with organization's risk profile, and in being able to show due care on behalf of the organization in the event of a compromise. CISO's look to consulting firms for maturity benchmarking, conferences for peer interaction, and vendors to help understand and develop their vision. These sources, while valuable, have significant flaws and inherent bias, yet they continue to be the primary sources of communication with cybersecurity program stakeholders regarding the security posture of the organization.

The need to effectively communicate the context of cybersecurity programs is further supported by the National Association of Corporate Director (NACD)'s "2019 Governance Outlook". In which The NACD report specifically called out to the need for boards to appropriately review the effectiveness of their organizations' cybersecurity management programs. Knowing the level of organizational integration between regulatory requirements and cybersecurity threats landed these two issues into top three trends concerning boards in 2019.

The four faces of the CISO

CISOs continue to serve the vital functions of managing security technologies (technologist) and protecting enterprise assets (guardian). At the same time, they are increasingly expected to focus more on setting security strategy (strategist) and advising business leaders on security's importance (advisor).

Technologist: The CISO as technologist guides the design, development, and deployment of secure technical architectures, instilling security standards and implementing innovative countermeasures. Technologists carefully select and implement platforms that support changing threat detection and monitoring solutions, and integrate services delivered by external sources into a seamless framework. Technologists ensure that architecture designs are flexible and extendable to meet future security and business needs. They develop and maintain the security policies and standards that an organization should adhere to, working with the CIO to ensure that platforms meet these requirements.

Guardian: As guardian, the CISO's charge is to monitor the effectiveness of the security program, processes, and controls in place. The guardian addresses considerations such as whether controls are

working as intended, data is secure, and information is properly shared. Guardians monitor processes that safeguard the confidentiality, integrity, and availability of data and drive the overall security program. They also measure and report on information security risks to keep stakeholders informed and meet compliance and regulatory requirements.

Strategist: As strategist, the CISO is the chief value architect for all cyber risk investments. The strategist partners with the business to align business and information security strategies and capture the value of security investments to safeguard enterprise assets. The strategist understands which business operations and information assets are critical, institutes strategic governance that prioritizes information security investments, and ensures that security and business resources and budgets are fully aligned to execute the priorities of the organization and deliver expected results.

Advisor: The CISO as advisor understands the implications of new or emerging threats and helps identify cyber risks that arise as the business advances new strategies. The advisor drives the enterprise to continuously improve its security decision-making and risk mitigation capabilities. The advisor understands where the organization needs to focus to address cyber threats and creates a risk-based strategic roadmap to align cybersecurity efforts with corporate risk appetite. Advisors possess significant political capital and are able to enlist, educate, engage, and align executive stakeholders to increase security awareness.

CISOs questions to shape the cyber risk organizational profile:

- What are the key drivers of value in the organization, and how are these being protected?
- What are the threats and vulnerabilities that provide the greatest exposure to us today?
- To what extent do we have the foundational capabilities and practices in place to protect our critical assets?
- How effective are the we at monitoring and detecting cyber incidents?
- Can we effectively respond to and recover from a cyber-incident? Do we have response plans in place, and have they been tested?
- What metrics demonstrates that we are effectively protecting the company?

How Smarter^{d} can help?

The good news is that, the Smarter^{d} Security Management Platform^{TM} addresses this critical gap in enterprise cybersecurity management through an innovative approach by continuously linking your cybersecurity capabilities to operational threat, vulnerabilities, business and IT capabilities, financial and market data directly to strategic cybersecurity planning decisions. Utilizing proprietary AI and ML techniques, the platform serves to provide holistic and integrated security program visibility around strategic cybersecurity risk posture and management priorities, plans, roadmap and budget.

Innovative Cybersecurity Risk Management Approach

Existing security management products focus on *either* operational or strategic risk – but typically fail to make a connection between the two. For example, Threat Intelligence (TI) platforms use their analytics to compute the risk of specific threat-vulnerability combinations and to prioritize vulnerability-remediation efforts, while Enterprise Risk Management (ERM) solutions focus on computing the business cost of data breaches. Neither of these approaches, however, by themselves provides analysts and decision-makers with sufficient context for cybersecurity action-planning.

Smarter^{d}, in contrast, builds on operational TI threat-and-vulnerability data, *processing it through an advanced cybersecurity knowledge-model to produce detailed, actionable recommendations* around the steps required to mature cybersecurity capabilities. In this way it provides more valid and practical risk management planning and decision-support than either TI or ERM approaches. The platform provides a subscription-based vehicle for dynamic, real-time and repeatable visibility into the maturity of cybersecurity programs using accepted standards like Top 20 CIS controls, NIST CSF, and ISO27001. The underlying knowledge model can easily be extended to encompass other cybersecurity control and compliance frameworks.

As our network grows our engine will dynamically learn and update industry benchmark for each control with other market data to help enterprise gain important contextual visibility. Gaining this kind of visibility via traditional methods is either very costly or time consuming or in some cases not available because of so many different reasons.

End-To-End Program Management Continuous Visibility

The challenge of managing multiple, simultaneous cybersecurity risk-reduction initiatives often constitutes a significant enterprise risk in its own right. Long-term efforts at maturing key cybersecurity capabilities, such as enterprise encryption or access management, often rise to the level of complex *programs* – encompassing multiple projects that involve competing resources and are subject to unexpected changes in the product-market landscape.

The Smarter^{d} security management platform is specifically designed to manage the challenge of multiple security initiatives by tracking project- and program-level dependencies including budget, vendor and contract and continuously alerting the decision-maker to emergent schedule risk.

Easy-to-Understand Security Management Dashboard

The Smarter^{d} security management platform is easy to use for both security analysts and executive decision-makers. Data-loading, knowledge modeling, AI/ML optimizations and risk computations are automated as background processes. What the end-user sees are statistical/graphical summaries indicating:

- Breakdown of risks posed by different combinations of threats and vulnerabilities
- Gaps in current cybersecurity capabilities, as measured by risk
- System-recommended roadmaps for cybersecurity capability improvement
- Detailed planning views showing project-level capability-maturity initiatives and interdependencies.

In addition, the end-user dashboard incorporates workflow management and fine-grained access control, to facilitate and securely manage the exchange of information among various platform users within an enterprise.

Communications and collaboration

CISOs can also struggle to communicate and collaborate with business leaders, in part because of limited interactions and relationships with them, a problem exacerbated by perception at the executive level. “As a result, most CISOs have to invest a lot of time to get buy-in and support for security initiatives.”

Those relationships are essential, though, in understanding what’s happening in the business and where the greatest risks lie. For example, since it is virtually impossible to protect every piece of data in an organization, a security leader needs to work with the business to understand which data is critical to the enterprise, where it resides, and the impact should it be lost or compromised. Based on this information security leader can determine what they need to do to protect the business and prioritize same. Smarter^{d} platform allows security team to capture/load all this information in single platform and effectively manage it.

Extensible Product Architecture

Smarter^{d} security management platform is a SAS-based solution that easily integrates with on-prem or cloud-based third-party threat intelligence feeds, asset repositories, project planning applications and third-party ERM applications – while providing secure segregation of customer data.

Simple Deployment Model

Smarter^{d} works with customers to address any integration requirements and provides initial training on utilizing the platform to improve operational efficiency and productivity, as well as leverage its AI/ML-based intelligence to improve strategic decision-making. Further details on the typical deployment tasks and timeline are available upon request.

Features

- ✓ Cybersecurity Posture
- ✓ Asset Management
- ✓ Vulnerability Remediation
- ✓ Incidence Remediation
- ✓ Compliance Management
- ✓ Assessment Management
- ✓ Roadmap Management
- ✓ Program Management
- ✓ Budget Management
- ✓ Vendor and Contract Management
- ✓ Dashboard and Reporting

Supporting Features

- ✓ Cybersecurity Control Framework (NIST, CIS, ISO 27001, CMMC)
- ✓ Support for Business and IT Capability Framework
- ✓ Asset Management (Support for Application, Software, Hardware and People)
- ✓ Ability to link and establish context across all elements of Cybersecurity Management
- ✓ Light-weight Risk Framework for Cybersecurity Control, Asset and Vendor Risk Management
- ✓ Built-in Collaboration to manage and track Features, Knowledgebase, Comments, Issues, Accomplishments, Kudos and Alerts
- ✓ Alerting Rules and Notification
- ✓ Sharing and Collaboration of Cybersecurity elements across the enterprise
- ✓ Standard Templates and CSV loaders for all required data
- ✓ Jira and Smartsheet Integration
- ✓ Email and Slack Channel notification
- ✓ Download data to CSV format
- ✓ Package and Component Level Access Control