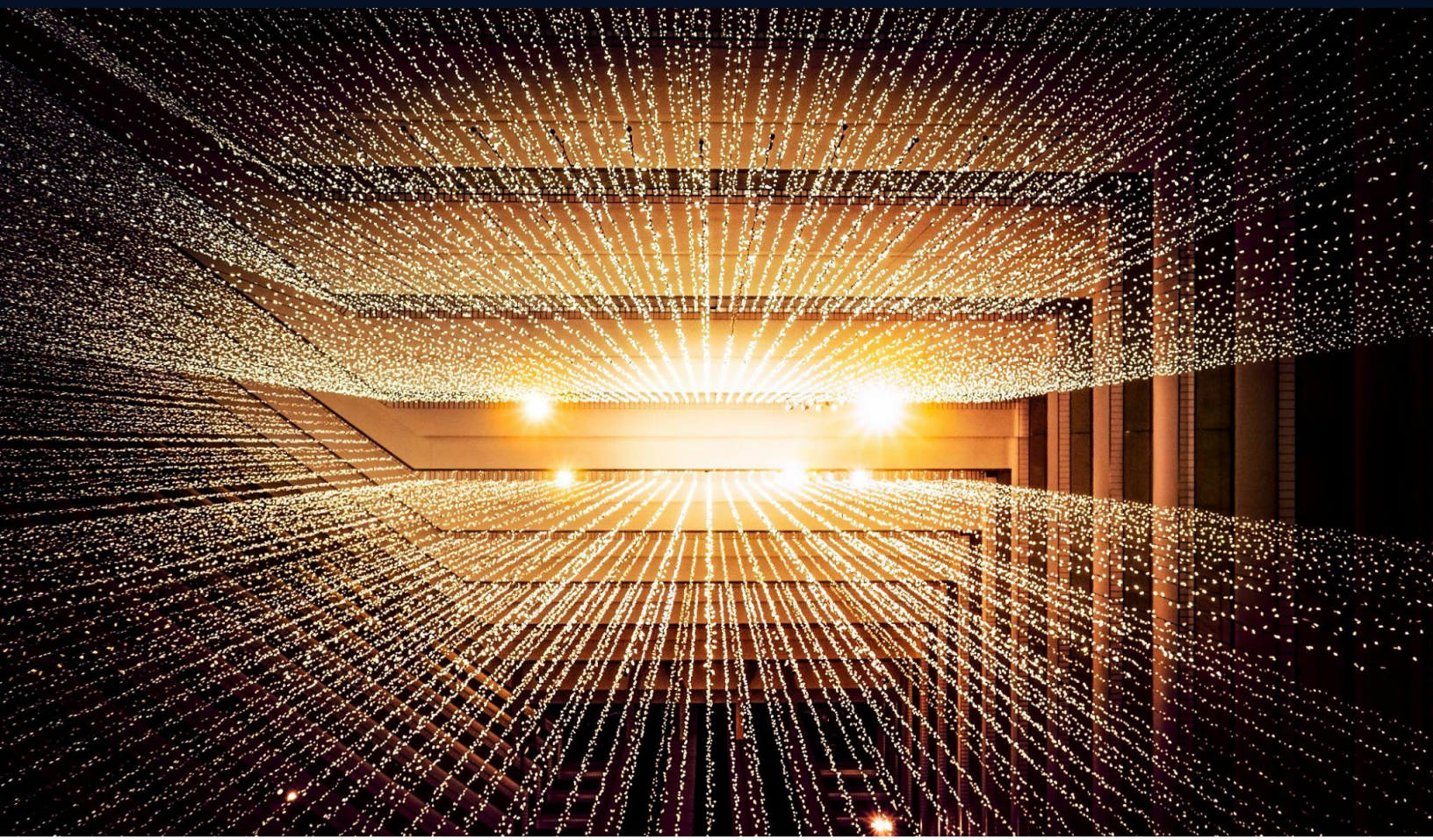
DAYBLINK CONSULTING

Cybersecurity Maturity Assessments

How DayBlink Consulting has conducted annual cybersecurity maturity assessments for a rapidly growing technology company



Introduction

A technology company faced significant challenges strengthening its cybersecurity posture to meet its rapid growth and position itself for IPO.

The newly appointed Chief Information Security Officer (CISO) had concerns about the maturity and sustainability of the company's security posture and requested a structured, comprehensive assessment to validate his perspective and address potential gaps.

The DayBlink Consulting team was engaged to assess, identify material maturity gaps, and help develop a long term security roadmap.

We built a methodology based on NIST CSF and a comprehensive maturity rubric to evaluate and improvement security practices.

Problem

The client faced significant challenges in preparing for growth due to a fragmented and inconsistent cybersecurity posture that lacked the maturity, scalability, and governance needed to manage enterprise-wide risk effectively.

While some security controls were in place, their implementation was uneven, and the deployment across the protect surface was inconsistent. This left critical areas exposed and made it difficult to ensure comprehensive risk coverage across the enterprise.

Compounding the issue, the Information Security (IS) team lacked the operational maturity and scalability needed to keep pace with evolving cyber threats or maintain resilience under sustained attack. Rather than being guided by centralized governance, the organization's risk management practices operated from the bottom up, with individual teams managing risk in isolation.

This fragmented approach made it difficult for leadership to determine if, and where, security investments were effectively reducing risk.

The client's security control coverage was widespread but lacked the depth and maturity needed to scale effectively

Emerging Security Practices: Security practices across all common security domains can best be characterized as partially implemented indicating they are "emerging" or on a path to "emerged"

Succeeding But Not Sustainable: With a relatively small IS Team, they were focused on daily maintenance ("fire-fighting") in the practices they have deployed and managed; it is challenging to sustain and harden practices

Growing Importance of Security: Cybersecurity is working its way into board-level discussions and updates, but is not yet risk-based, hardened and institutionalized

Fragmented & Inconsistent: While security domain coverage is high, implementation levels and protect surface coverages, are fragmented and inconsistent when looking across business units

Not Scalable: The IS Team is not positioned well to scale and mature cybersecurity practices to protect against an advanced cyber threats nor remain resilient under attack

Limited Top-Down Strategy: Security risk management practices are bottoms-up vs. strategically defined top-down. This structure makes it difficult to understand if security investment is reducing security risk holistically

Solution

Our team successfully developed a maturity model based on NIST's Cybersecurity Framework (CSF) to evaluate, baseline, and improve target areas.

To address our client's cybersecurity challenges and its unique environment, we developed a custom maturity model using NIST's CSF as its core with elements of C2M2 and BSIMM. This allowed for a structured and scalable approach to evaluating the organization's cybersecurity capabilities.

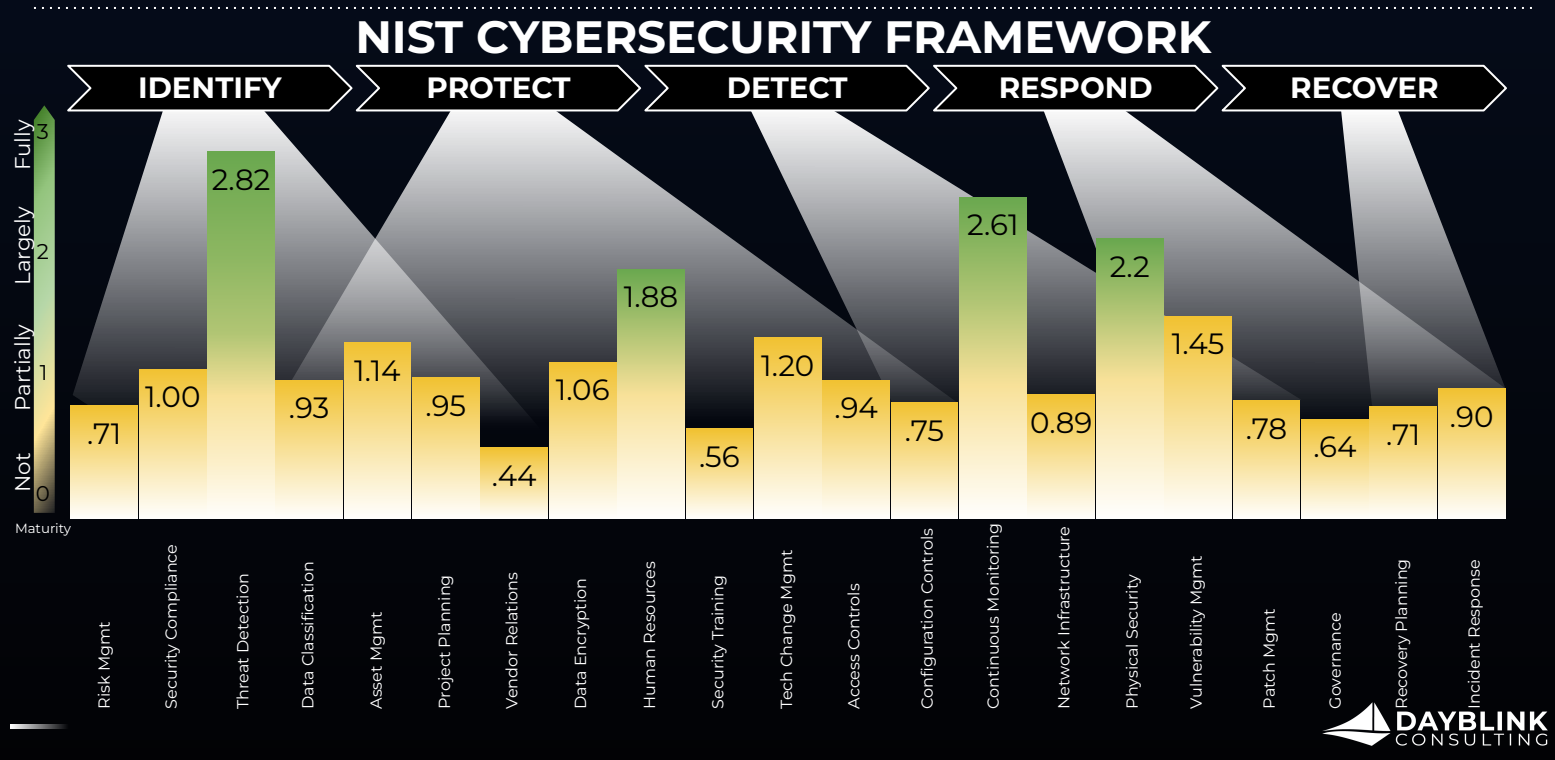
The team created an evaluation rubric to assess the security controls across all business units. This rubric ensured consistency in evaluating controls and enabled comparison across functions.

Maturity levels were defined using a scale from "partially implemented" to "fully implemented," providing clarity on where the foundational elements existed and where major gaps remained.

To enhance the precision of the assessment, maturity was further refined by evaluating the operational status of key maturity indicators i.e., the existence and comprehensiveness of: Program, Strategy and Plan; Governance; Policies and Standards; Processes and Procedures; Automation and Tooling; Metrics and Reporting; Resource Allocation; and Protect Surface Coverage.

This detailed approach enabled the team to clarify if the control existed, but also to understand the depth of its deployment or adoption and its effectiveness across the organization.

Finally, the team established a repeatable annual assessment process that informed long-term strategic planning, gave leadership visibility into enterprise risks, and guided high-impact investments to mature cybersecurity in line with growth and risk goals.



DAYBLINK CONSULTING

Outcome

The team adopted the focused roadmap to strengthen the overall security posture

DayBlink Consulting identified and catalogued 151 specific gaps and improvement opportunities. These ranged from weak control implementations, inconsistencies in operational practices to information security functions not yet in place.

Example opportunities included (1) Create Shadow IT Discovery Program, (2) Implement Mobile Device Management (MDM) Program, (3) Develop a Comprehensive Role Based Security Awareness and Training Program, (4) Refine Vulnerability and Patch Management Processes, (6) Enhance Data Protection and Loss Prevention Controls, (7) Enforce Secure Configuration and Change Management Practices, (8) Establish a BCDR function, (9) Conduct Security Assessments and Penetration Testing.

Each opportunity was t-shirt sized based on impact to the maturity score and level of effort. We then built a phased roadmap that outlined near-term wins and long-term goals, enabling the organization to make steady, measurable progress in improving maturity scores over time.

151

Total Gaps Identified

45

Material Maturity Gaps

30

Strategic Initiatives Recommended

WASHINGTON D.C. (Headquarters)

8609 Westwood Center Dr., Suite 110,
Tysons Corner, VA 22182

CONTACT US

Jacob Rosner, Manager
jacob.rosner@dayblinkconsulting.com

DAYBLINK CONSULTING

www.dayblinkconsulting.com