BLUELAVA

CASE STUDY

CYBERSECURITY MATURITY ASSESSMENT

Assessing Your Program Maturity for Credibility and Impact Over Time

Measuring how well the company is protected and having visibility into how that changes over time is critical to guiding future decisions. So, when this established CISO was brought in to take over the security program of a recent divestiture, he invested in the Blue Lava Security Program Management platform.

RESULTS	BEFORE	AFTER BLUE LAVA
Data Quality	Subjective, unstructured, and not in the business language	**Evidence-based in business language; 20% more coverage**
Time-to-Value	"Non-existent"	**10X faster, more prescriptive guidance for future discussions**
Reporting Efficiencies	Manual, spreadsheet-driven	**Automated, data-driven, instantaneous**

Customer Profile

- An experienced CISO from one of the largest global medical products companies with more than 11,000 employees and 120 offices across the globe
- The CISO needed to quickly assess his newly inherited security department, at the time undergoing a digital transformation

Challenge

As a recent spin-off from a larger conglomerate, the legacy IT operations were centrally managed. Being the first dedicated security department, the team lacked a formal cybersecurity program. Any evaluation of the cybersecurity program prior had been managed through the former parent company compliance department, which focused primarily on adhering to regulatory requirements (PCI, SOX, HIPAA, GDPR, etc.). Not only was it challenging to depend on an enterprise assessment conducted for other purposes, it did not adequately measure the company's true security posture.

As with all organizations undergoing digital transformation, this medical device manufacturer was moving online, which comes with increased business and cybersecurity risks. The CISO needed to level-up their security program for operations and supply chain in order to satisfy customers' ever-demanding supplier risk and certification requirements.

This CISO knew without a baseline of what he inherited (what he had and what he didn't have); he would not be able to establish a successful plan and roadmap necessary to properly protect the organization. The CISO also needed to establish the credibility of the program - internally with business stakeholders and externally with prospects, customers and

> *...In the process of creating a baseline maturity assessment, we were not only able to develop a strategic roadmap based on our top findings, but it really helped establish a new mindset as a cybersecurity team.*
>
> **CISO, Global Medical Supplies Company**

partners. As a critical and immediate first step, he needed to conduct a proper maturity assessment. In order to accelerate and automate this process, he invested in the Blue Lava Security Program Management (SPM) platform.

Solution

Through this exercise of establishing a baseline, the CISO was able to uncover several areas of potential vulnerability and begin a dialogue with the company Executives. As a result of having the necessary data to have a business discussion, he was able to have more productive conversations with the C-Suite and Board around current gaps and proposed solutions moving forward.

Better Cybersecurity Program Maturity Assessment

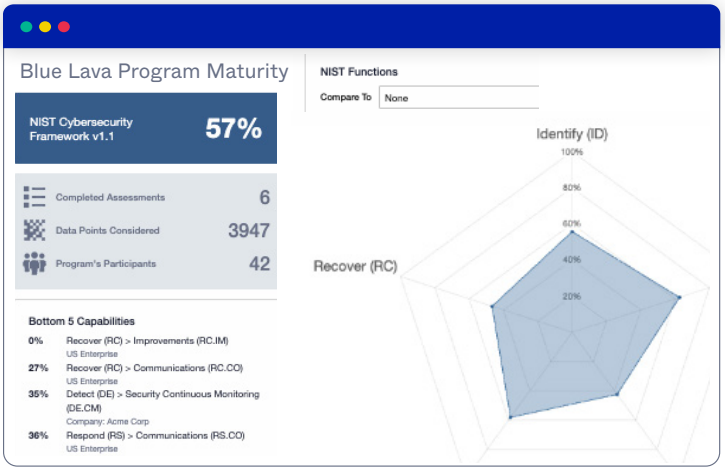
By collecting and storing assessment inputs, the team has been able to produce a consistent, repeatable process. This approach created a living record of all assessments, improvements, and program decisions to better prioritize and measure the impact and effectiveness of the security program over time.

No longer depending on assessments made for other purposes like compliance, the CISO is able to provide a much deeper, more advanced, and comprehensive understanding of the company's security posture. The CISO began to establish a maturity score with clear accountability organization-wide, to maintain and improve upon the cybersecurity program over time.

He was also able to provide strategic direction for the business by conducting a foundational assessment of a recent company acquisition. Armed with a repeatable framework, he was able to review the data of the acquired organization's security program to plan and anticipate investments for the migration.

Moving forward, the CISO plans to continually refine the program by establishing future maturity score goals, prioritizing security initiatives based on findings and aligned to business growth objectives.

Leverage automated mapping to NIST-CSF



BLUELAVA

Blue Lava empowers you to effectively communicate priorities, needs, recommendations and results to your larger community of business and finance stakeholders, pivoting from reactive to proactive decision making. Communicate security program results and needs to business stakeholders with consistency and ease.

Learn More