At-A-Glance

Benefits

- **Evaluate and improve** your organization's cybersecurity management program and underlying controls
- **Identify** security gaps, ineffective operational processes and poorly designed technology security controls
- **Define** a security strategy and roadmap to address current and emerging threats
- **Develop and prioritize** security improvements to maximize return on your investment and better protect your data

Cisco Cybersecurity Management Program Assessment

Security is now a boardroom issue. As organizations become digital and explore growth strategies tied to embracing new technologies, their attack surface expands. According to Accenture, an organization faces an average of one hundred attacks per year, with internal security teams only finding approximately 65% of those.[1]

The Challenge with Cybersecurity Programs

With the fast pace of technology and an ongoing shortage of security talent, many organization's cybersecurity teams continue to struggle to effectively communicate cybersecurity issues to senior leadership. This challenge is most often revealed in grassroots cybersecurity initiatives that have evolved into corporate cybersecurity programs. Typically, this resulted from an enterprise implementing solutions to specific technical challenges, as opposed to strategically addressing security as it relates to business objectives. No longer effective as a point solution, cybersecurity management has become a business function with greater level of integration into other business units and can underpin performance outcomes.

Cybersecurity as a Business Function

To support a holistic and comprehensive view of an organization's security posture, our security advisory consultants help you understand your current security posture, work with you to determine your target state taking into account your current investment, and then recommend cost-effective improvements designed to help you reach your target state. We design our recommendations around the following key success factors:

- Support and drive strong governance attitudes and actions
- Designed, developed, and implemented in a similar way to other business functions
- A standard framework approach usable for an extended period of many years with little to no changes
- Measurable in terms of its effectiveness.

[1]Page 2; Building Confidence: Facing the Cybersecurity Conundrum. Accenture, 2016.

© 2016

Cisco Cybersecurity Management Program Assessment

Through Cisco's unparalleled experience, expertise, and understanding of what works in the "real world", Cisco's Security Advisory Services team helps our customers to assess and develop plans to secure their data against complex adversaries while aligning security goals and controls to business strategies. Cisco will review your cybersecurity management and governance structures, the effectiveness of your organizational design to support cybersecurity goals, the operational processes that manage technology and support cybersecurity, and the effectiveness of the cybersecurity technology controls.

We develop a roadmap for your use to help you reach a target security posture and level of maturity appropriate to your business and the threat environment you operate in.

Next Steps

Visit www.cisco.com/go/securityservices to connect with our advisors and protect your business today.

Case Study:

Challenges

- Inability to accurately rate cybersecurity program maturity hindering negotiating ability during merger/acquisition negotiation.
- Inability to determine whether cybersecurity controls are sufficiently mature nor how they rate when compared to industry peer group.
- Inconsistent and unconsolidated software and hardware asset management
- Inconsistent cybersecurity policy, standard, and procedure documentation made it difficult for staff to find the appropriate information when necessary, leading staff to perform using ad-hoc processes.
- No Cloud strategy despite several SaaS services already in use.

Solutions

- Perform a Cybersecurity Management Program Assessment to determine the maturity of the overall cybersecurity management program, and it's policies, standards, and procedures
- Work with customer to determine target maturity for each, and develop an improvement roadmap for customer to use to address maturity gaps between current and target maturity
- Improvement roadmap includes:
    - Long-term effort to build consistent software and hardware asset management via interface with Procurement Process and Network Access Control.
    - Establish documentation standard, annual document review, and implement a searchable intranet-based document repository.
    - Develop and implement public and private Cloud strategy and Cloud Services Catalog, managing internal server environment as Private Cloud.
    - Establish a metrics and reporting capability within Compliance to work with executive leadership to determine the messaging that is important to them, develop reporting capability to meet needs, and implement periodic review.

Outcomes

- New security model and architecture enable rapid innovation in a growing market and flexibility to address merger and acquisition activity.
- Improved compliance and consistent detailed process work through improved policy, standard, and procedure availability.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

12/12/16