Gartner Research

How to Build a Robust, Defensible Security Program That Enables Business Growth and Agility

By Tom Scholtz

23 February 2022

How to Build a Robust, Defensible Security Program That Enables Business Growth and Agility

Published 23 February 2022 - ID G00766390 - 7 min read

By Analyst(s): Tom Scholtz

Initiatives: Cybersecurity Leadership

Effective cybersecurity is predicated on a defensible security program. Cybersecurity leaders should use this research to understand the characteristics and build a continuous security program that is defensible and ensures a balance between protection and the need to run the business.

Overview

Key Findings

- Senior executives are coming under increasing governance pressure to demonstrate that the organization is practicing due diligence in dealing with cybersecurity threats and risks.
- Security programs often lack appropriate defensibility at the business level, leading to mistrust and inappropriate business support and investment.
- Many security programs still focus on ticking compliance boxes to the detriment of the ability to implement effective, risk-based security controls.
- Business leaders continue to treat security as a business inhibitor due to the lack of a defensible security program that links into business outcomes.

Recommendations

To achieve a defensible information security management program, cybersecurity leaders should:

- Ensure clear accountability for information risk to enable effective risk-based control decisions.
- Build a program that reflects the unique business context of the organization, leveraging generally accepted standards and proven practices.

- Engineer the program for agility and continuous improvement by, among other actions, emphasizing key principles and formalizing security processes.

Introduction

The only way to deal effectively with the evolving risks of digitalization and increasing cyberthreats is to institute a continuous security program. Unfortunately, too many organizations just “tick the boxes” when they aim to establish a security capability — that is, they typically produce a lot of documentation and invest aggressively in technology. But they spend little or no time on establishing effective governance, or the ability to assess and interpret risk effectively.

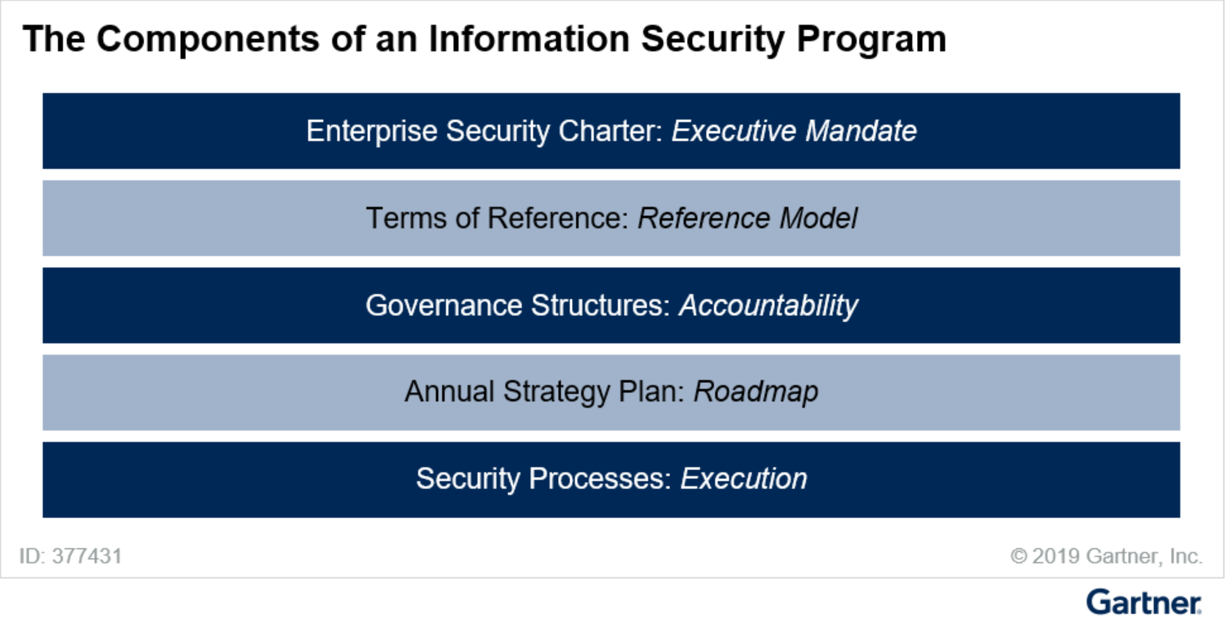
A defensible security program substantiates the answer to the important question from stakeholders: “Is the organization doing enough to reasonably protect its information resources?”

To be defensible, a security program must:

- Have a clear mandate from executive leadership
- Establish and enforce clear owner accountability
- Invest in risk assessment capability
- Reference accepted standards (while avoiding mindless compliance)
- Be clearly linked to the unique business context of the organization
- Support digitalization strategies
- Focus on continuous improvement
- Be agile enough to respond fast to changing threats and scenarios
- Support formal, repeatable security processes

Figure 1 shows the components of a typical information security program in an organization. In this research, we expand on the best practices CISOs should adopt to make a security program defensible.

Figure 1: The Components of an Information Security Program



The Components of an Information Security Program

Enterprise Security Charter: *Executive Mandate*

Terms of Reference: *Reference Model*

Governance Structures: *Accountability*

Annual Strategy Plan: *Roadmap*

Security Processes: *Execution*

ID: 377431

Source: Gartner (February 2022)

Analysis

Ensure Clear Accountability for Information Risk to Enable Effective Risk-Based Control Decisions

The foundation of a defensible security program is the Enterprise Security Charter. This is the short document, written in plain language, which establishes clear owner accountability for protecting information resources, and provides a mandate for the CISO to establish and maintain the security program. This charter document must be read, understood, signed off, visibly endorsed and annually reaffirmed by the executive leadership (for example, the CEO and board) of the organization.

A key aspect of defensibility is the ability to support risk-based control decisions. At a minimum, this entails having a risk register with the associated process for identifying and capturing risks, assigning ownership and tracking remediation. If the resources are available, this risk management process must also include the adoption and customization of appropriate risk assessment methodologies and tools, with the requisite trained specialists, to perform ad hoc and periodic risk assessments. Proper documentation of risk management activities and decisions is an implicit part of defensibility. Once a risk is identified, all the associated aspects (such as assessed exposure, owner, mitigation decision and mitigation actions) must be formally documented.

Many regulations require a formal, staffed CISO, with appropriate independence from information resource owners. In resource-constrained organizations, or those going through major transformations or merger and acquisition (M&A) activity, a virtual CISO position can be an acceptable compromise. If the size of the organization, the maturity of the security program and the cultural and political realities allow for it, the CISO function should report independently from the CIO. While this separation in itself raises some challenges, it does support defensibility from a corporate governance perspective.

Security decisions cannot be made in isolation by the security team. An information security steering committee (ISSC) with direct, decision-making representation from information owners (business units) and staff functions (legal, HR and privacy office) can be an effective forum for discussing security challenges, proposed policies and investment plans. It is an essential forum for soliciting ongoing input and support for the security program from senior business leaders and for ensuring that these leaders are aware of the risks in not only their own business unit but also across all businesses.

A key element of defensibility is credibility. Executive reporting frameworks and processes can be effective tools for establishing and maintaining the credibility of the program. The framework and associated process must report security program and risk posture status in a manner that allows for informed, risk-based executive decisions to be made. As far as possible, it must indicate the impact of security risk on the ability of the organization to achieve its business KPIs. Reporting technical details, like the number of blocked spam messages, does not contribute to business objectives.

Build a Standards-Based Program That Reflects the Unique Business Context of the Organization

A prerequisite for getting business support for the security program is a clear vision that conveys the components and objectives of the program in terms that nonsecurity specialists can understand and executives can subscribe to.This vision should be relevant to the business context. It must reflect the business, technology and environmental drivers that are unique to the organization (see Table 1).

Table 1: Examples of Business, Technology and Environmental Drivers That Influence an Organization's Security Vision

Business Drivers	Technology Drivers	Environmental Drivers
Cost-cutting programs, product diversification, geographical expansion, M&As and divestitures	Digitalization strategy, data center consolidation and cloud adoption	Regulatory requirements (such as the GDPR) and major cybersecurity threats

Source: Gartner (February 2022)

A key element of defensibility is the ability to demonstrate that the organizations' efforts are in line with generally accepted proven practices and standards. With respect to the security program, this means using one or more taxonomical reference models, based on accepted industry standards (such as the NIST cybersecurity framework [CSF], ISO/IEC 27001/2 or CIS Controls [formerly known as Critical Security Controls]) to guide strategic and tactical decisions.

Many organizations utilize peer benchmarking of various elements of their program (for example, level of spend, number of staff, program maturity or levels of compliance with generally accepted standards) to support their argument for defensibility.

Another element of defensibility is an annual security strategy plan that clearly reflects the midterm to longer-term business needs for security. This means that the plan:

- Articulates the strategic vision and business context (the changing business, technology and environmental drivers) mentioned above.
- Leverages multiple assessments (for example, maturity assessments, vulnerability assessments, risk assessments, audit findings, and penetration tests and/or compliance assessments) to provide different perspectives on the current state of the organization's security capability.
- Provides a prioritized roadmap that clearly links projects and corrective actions to the gaps, risks or vulnerabilities identified in the assessments, and to the relevant business, technology and environmental drivers.

For organizational leaders to embrace and support the security program, which is a clear demonstration of defensibility, security policies must be socialized with, and reviewed and approved by, the business leadership that will be subject to these policies. These aspects should be formally integrated into the policy management process, and the ISSC should be leveraged to review, discuss and approve security policy in a collaborative manner. Also, security policies must be formally documented, disseminated and communicated via the security awareness program.

Engineer the Program for Agility and Continuous Improvement

Effective security is a continuously moving target. Recognizing and planning for this reality is an illustration of defensibility. The security program must be geared toward anticipating and reacting to frequent, unexpected changes in the business, technology and operating environments, as well as driving continuous improvement in the effectiveness and efficiency of security controls.

The ability to continuously improve while simultaneously reacting to change predicates a set of commonly agreed security principles that guide security planning, implementation and operations on a day-to-day basis. Examples of such principles include:

- Making controls decisions based on specific risk and risk appetite rather than on check-box compliance.
- Supporting business outcomes rather than solely protecting the infrastructure.
- Ensuring the role of the human element is always considered when designing and managing security controls.

Additional characteristics of defensibility regarding agility and continuous improvement include:

- Regular/periodic vulnerability assessments of the organization's environment, potentially linked to the utilization of threat intelligence if the resources are available.
- A continuously evolving security monitoring and detection capability, linked to an incident response process that is regularly tested.
- A continuous user awareness and training program, with user awareness and knowledge levels tested regularly.
- Clear ownership of defined security processes (such as risk management, policy management, threat and vulnerability management, and identity and access management) with their associated RACI charts.

Evidence

More than 400 Gartner client inquiries on security program management and strategy planning between January and December 2018

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Institute Cybersecurity and Risk Governance Practices to Improve Information Security

Best Practices for Establishing an Information Security Steering Committee

Security Management Strategy Planning Best Practices

Toolkit: Information Security Strategy on a Page — Deconstructed

Security Program Management 101 — How to Select Your Security Frameworks, Controls and Processes

Security Fundamentals — The Services and Processes You Must Get Right

Outcome-Driven Metrics for Cybersecurity in the Digital Era

Actionable, objective insight

Position your IT organization for success. Explore these additional complimentary resources and tools for security and risk leaders:

Webinar

The Gartner Leadership Vision for 2022: Security and Risk Management

Prioritize your time and energy with top-level guidance based on our data-driven research.

Watch On Demand

eBook

Four Facets of Effective CISO Leadership

Discover how best-in-class cybersecurity leaders tackle their expanding remit.

Download eBook

eBook

3 Must-Haves in Your Cybersecurity Incident Response Plan

Improve your organization's ability to be prepared for a cybersecurity incident.

Download eBook

Research

Top Trends in Cybersecurity 2022

Explore the 12 trends shaping the future of digital business.

Download Research

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight to deliver on your mission-critical priorities. Our expert guidance and tools enable faster, smarter decisions and stronger performance. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for IT Leaders
gartner.com/en/information-technology

Stay connected to the latest insights