How to Communicate the Value of Information Security in Business Terms

Published 9 July 2020 - ID G00728406 - 10 min read

By Analysts Tom Scholtz

Initiatives:Security and Risk Management Leaders

Despite higher levels of awareness regarding cybersecurity risk, executive leaders responsible for information security find it difficult to articulate its benefits. Given its importance, they must ensure that those benefits are communicated in the relevant business terminology.

Overview

Key Challenges

- Presentations of security investments by security leaders are seldom connected to revenue increases or cost savings.
- Despite the continuing high levels of publicity about cybersecurity incidents, most organizations still view information security cost as a necessary evil rather than a business investment.
- Information security presentations often don't resonate with cross-functional leaders and the board.

Recommendations

Executive leaders looking to ensure information security strategies are aligned with business strategy must:

- Adopt a business value model (such as Gartner's 4I Model) by outlining expected business values in a consistent format.
- Ensure that information security strategy is linked to business strategy by identifying relevant business drivers and mapping them to the business values articulated in the model.
- Ensure security leaders gain support for the information security strategy by making sure that proposed actions (with their expected costs), relevant business drivers and expected business value are always presented to peers and the board.

Introduction

This research is adapted from "Articulating the Business Value of Information Security," which guides information security teams on how to demonstrate the business contribution of their

activities and plans to get funded.

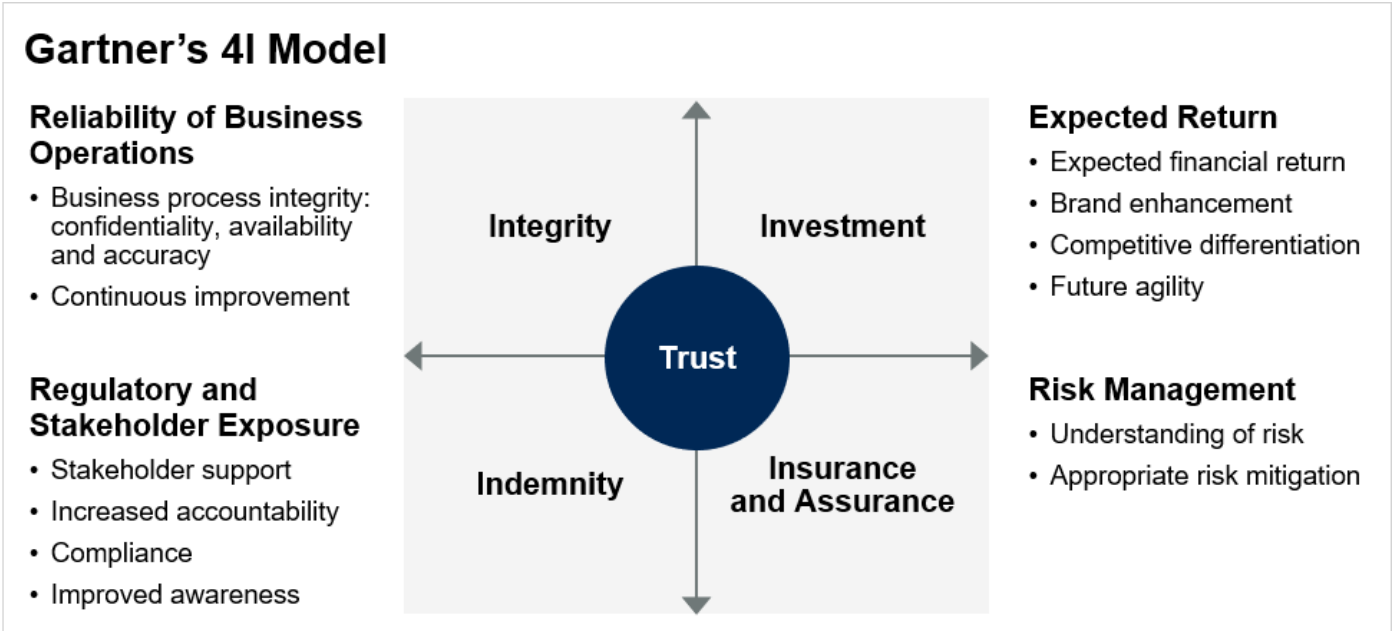
Organizations find it challenging to articulate the benefits of information security (increased confidentiality, integrity and availability — typically referred to as the CIA triad) and obtain and maintain their employees' and board's support for information security strategies. The fact that justification messages are usually constructed around negative themes (scare statistics, inflated risk exposures and impending disasters) does little to further the cause. This is because the focus is on risk avoidance rather than business outcomes; thus, negative messages are often perceived as counterproductive and obstructive.

Therefore, articulating the value of information security program in business terms is imperative — as initiatives that cannot demonstrate clear business value will not be funded.

The best vocabulary for articulating business value is, of course, financial. One obvious approach to expressing the value of information security is to see it as insurance. Insurance works with historical damage data and risk triggers to determine appropriate premiums. Unfortunately, consistent historical damage and risk trigger data are not readily available for specific information security incidents. Hence, it is difficult to proactively quantify the financial return on investment resulting from most information security expenditures.

Executive leaders play a crucial role in ensuring their teams evolve alternative mechanisms for capturing and articulating value of their information security program. At a project level, the best approach is to use a balanced cost-benefit analysis based on expected impacts and articulate the benefits as risk reduction, quantifiable financial returns and other expected improvements. However, this approach is too granular to use effectively at a more strategic level (e.g., when going to the board of directors to obtain strategic support and investment for the information security program). What is required at this level is an approach for transcribing the strategic benefits of information security into business value. We recommend using Gartner's 4I Model (see Figure 1).

Figure 1: Gartner's 4I Model



Source: Gartner
ID: 407639

Analysis

Adopt an Information Security Business Value Model Outlining Expected Returns

Organizations need to develop a model for articulating information security benefits into business value messages. Gartner's 4I Model (see Figure 1) describes four dimensions against which the business value of investing in strategic information security activities can be captured, summarized and communicated in a concise format:

- **Integrity,** which emphasizes the impact of the reliability and availability of daily business operations. The benefits are manifested as continuous improvements in the confidentiality, availability, and accuracy of business information and processes.
- **Investment,** which captures the expected returns. The value typically can be articulated as expected financial returns, brand enhancement, competitive differentiation, future agility, organizational adaptability.
- **Insurance and assurance,** which address the risk management benefits. These result from an increased insight into the information risk factors facing the organization, resulting in more effective and appropriate risk identification, assessment and management activities. Risk management options include accepting, avoiding, transferring, mitigating or ignoring assessed risks.
- **Indemnity,** which highlights the compliance benefits of limiting regulatory and stakeholder exposure. This results from improved awareness, increased accountability, greater stakeholder support and, consequently, improved legal and regulatory compliance.

At face value, these value components do not seem to be much different from the traditional CIA messages, but they subtly express the positive outcomes of investing in security in a manner that relates to business challenges. When articulating the business value expressions, executive leaders should encourage their direct reports to review the terminology and have suggestions to make it relevant to the business.

The business value expressed in the four dimensions can be summarized as an expression of trustability. Preferably, the organization should have some specific goals for trustability. In most organizations, these goals exist but are not clearly articulated. Taken together, the outcomes of the security program will greatly contribute to improved trust in the organization among customers, partners, employees and other stakeholders.

Link Information Security Strategy to Business Strategy by Identifying Business Drivers and Mapping Them to the Business Values Articulated in the Model

Executive leaders should check that the information security strategy captures existing business drivers that manifest themselves in the organization. These drivers should relate to actual business strategy and associated initiatives.

The key messages regarding security value must be related to the organization's business strategy. Most commercial organizations have a fundamental strategy based on one (or maybe a combination of two) of the following:

- Service leadership (having better customer relationships than the competition)
- Quality leadership (being better than the competition)
- Price leadership (being less expensive than the competition)

Basic business strategy theory states that a commercial organization must excel in one of the three and can be above average in a second, but it is impossible to lead in all three and any attempt to do so will lead to failure. Executive leaders should ensure that the information security strategy and its underlying business value expectations support the business strategy. This does not necessarily imply a direct, one-to-one linkage between strategies — that is, supporting a business strategy of price leadership (being less expensive) might actually require an IT and information security strategy based on quality (being better). In such a case, a modern, robust, secure IT environment enables price competitiveness.

A simple technique entails identifying specific business initiatives that are being executed in support of the business strategy and linking the security message to such initiatives. Examples of such business initiatives could be the development of new products or services, new product delivery models, cost-cutting projects (such as office and data center consolidation), or merger and acquisition activity. By analyzing the motives behind a given business initiative and understanding how it will contribute to the overall business strategy, it becomes easier to identify the relevant, associated business drivers for information security. For example, if the business embarks on an aggressive strategy to increase its market share, this will have implications for the confidentiality of product and marketing plans, acquisition plans, or geographic expansion plans.

Good sources for business initiatives include strategic business plans, executive communications, annual reports and interviews with selected executives. Typical examples of business-initiative-based drivers include:

- **Product brand and resource protection.** Product brands have inherent value and are exposed to competitive or malicious damage to the resources (intellectual property and knowledge) associated with the respective brands.
- **Protecting and enhancing the corporate brand and its associated values.** These include preventing the negative impact on the value of the business and its corporate image as a result

of security incidents. They also include brand enhancement through proactive action (for example, by establishing an image of trustworthiness, good citizenship and governance).

- **Supporting the market share strategy.** Breaches of sales or product strategy information can be detrimental (for example, the compromise of product launch plans can have a serious impact on timeliness and competitiveness).
- **Business process availability.** Over and above the obvious importance of customer-facing processes, the impact on back-end processes (for example, financial systems and supplier interfaces) must be taken into consideration.
- **Agility and adaptability.** The need to respond faster to changes in the business and technology environments, and the ability to securely exploit technology to develop new products and channels.
- **Improved insight into the costs and benefits of security investments and activities on a continuous basis.**
- **Global and local trends in information security.** Keeping abreast of security investment trends, best practices and approaches, executive focus, and the use of information security as a business differentiator.
- **Lessons from the past.** Any recent security incidents that impacted the enterprise (for example, the impact of recent virus/worm attacks, website hacks, internal security lapses, fraudulent activities and audit reports).
- **Changes in the regulatory environment.** Responding to the security implications of any changes in laws or regulations (for example, corporate governance, privacy, audit, disclosure/transparency legislation or regulation; sector-specific legislation; and e-signature/e-commerce/e-business regulation).
- **Changes in the business environment.** Responding to security implications of changes in the business environment (for example, geopolitical risks).

Once the relevant drivers have been captured and articulated, they can be mapped to the most appropriate business value categories in a business value table (see Table 1). Table 1 is an example that outlines **what** needs to be done (the recommended projects and initiatives), **why** it is important to take these actions (the relevant business drivers) and what the **expected business value** of these activities is.

Table 1: Sample Information Security Business Value Table

↓	*Investment* ↓	*Integrity* ↓	*Insurance/Assurance* ↓	*Indemnity*

	Investment	*Integrity*	*Insurance/Assurance*	*Indemnity*
Definition	■ Expected returns	■ Reliability of business operations	■ Risk management	■ Regulat and stakeho exposu
Business Value	■ Expected financial return ■ Brand enhancement ■ Competitive differentiation ■ Future agility	■ Business process integrity: confidentiality, availability and accuracy ■ Continuous improvement	■ Understanding of risk ■ Risk and cost avoidance ■ Appropriate risk mitigation or acceptance	■ Increas accoun ■ Compli ■ Improv awaren ■ Stakeho support
Relevant Business Drivers	■ Corporate profile and name ■ Market share strategy ■ Lack of cost/value insight ■ Agility and adaptability ■ Warnings from the past ■ Regulatory environment	■ Product brand and resource protection ■ Market share strategy ■ Business process availability ■ Warnings from the past	■ Product brand and resource protection ■ Corporate profile and name ■ Lack of cost/value insight ■ Warnings from the past ■ Regulatory environment	■ Corpora profile a name ■ Global a local bu trends ■ Regulat environ

	Investment	Integrity	Insurance/Assurance	Indemnity
Requirements/ Recommended Actions	■ Coordinated information security strategy plan ■ Guidelines for selecting appropriate security solutions ■ Common mechanism for articulating value of security	■ Security awareness, behavior and cultural improvement ■ Appropriate, specific security policies ■ Identification and implementation of security operations processes ■ Alignment (and rationalization) of security technology	■ Risk management as a core competence ■ Common risk management strategy, methodology and toolset	■ Risk manage alignme ■ Compli function process ■ Security process practice alignme

Source: Gartner

Requesting input from key stakeholders (such as key members of the enterprise security steering committee) when constructing this table will help with validating and contextualizing the messaging.

Gain Support From Board and Peers by Communicating Proposed Actions, Relevant Business Drivers and Expected Business Value

In itself, Gartner's 4I Model does not provide a panacea for successful communication. The business value articulated via the model must be communicated in a format that will be accepted and assimilated by the cross-functional peers and board. This could take the format of a presentation, a strategy document, a memorandum or any other appropriate mechanism. It should include a summary of estimated costs and resource requirements, and a high-level indication of the expected duration of the combined activities. Using basic communications and marketing principles, the message must be tempered by the audience's characteristics and by corporate cultural realities.

Major obstacles to effective communication include:

- **A lack of accountability ownership among cross-functional peers for managing the risks of their information resources.** This is primarily a governance issue, but it is important to understand the status quo regarding risk ownership to improve the chances of successful communication.
- **The lack of formal corporate trustability goals.** For example, Company XYZ wants to be a trusted e-commerce provider, and it will strive to achieve and maintain an overall maturity level of four for its information security program. If the organization has not adequately dealt with its own corporate trustability goals, then it will dilute any attempts to communicate business value. Therefore, it is important for an organization to explicitly define its risk management and trustability goals.

In addition to effective communication, it's imperative for executive leaders to build credibility regarding information security programs with peers and the board to obtain and maintain their support.

A key component of maintaining credibility is to provide continuous, honest feedback on security activities and achievements, and specifically to compare actual results with expected benefits. This should be done at all levels of security and risk management activity:

- Project (project results)
- Program (status and progress reporting)
- Operational (process and status metrics)
- Strategic (security and risk scorecards)

Evidence

The research is based on 1,021 Gartner client inquiries on security program management and strategy planning conducted between August 2018 and July 2019.

Recommended by the Author

The Characteristics of a Defensible Security Program

Top Tips for Communicating Security and Risk to Business Stakeholders

Recommended For You

Articulating the Business Value of Information Security

Know Your Personality: Decrease Your Information Security Vulnerabilities

Product Security: CISOs' Secret Weapon for Adding Value