Cybersecurity Must Be Treated as a Business Decision

Published 14 July 2020 - ID G00731758 - 15 min read

By Analysts Paul Proctor

Initiatives: IT Cost Optimization, Finance, Risk and Value

Lines between business models and the supporting technologies are blurring. Executive leaders should work with their peers and direct reports to overcome the typical cybersecurity pitfalls and achieve their digital business goals.

Overview

Key Challenges

- Cybersecurity spending growth is slowing through 2023, while boards are starting to push back and ask what they have achieved after years of heavy cybersecurity spending.

- Boards and executive leaders are asking the wrong questions about cybersecurity, leading to poor investment decisions.

- Many current approaches to improve cybersecurity are falling short of providing appropriate and defensible levels of protection.

Recommendations

Executive leaders involved in addressing cybersecurity risk should work with heads of risk and assurance functions to:

- Use this research to build a business case and board narrative to change how cybersecurity is treated in the organization.

- Ensure their organization’s cybersecurity readiness is improved by treating it as a choice and a business decision.

- Establish cybersecurity priorities and investments by using an outcome-driven approach that balances investment and risk with the needs to achieve desired business outcomes.

Introduction

This research is adapted from “The Urgency to Treat Cybersecurity as a Business Decision,” which guides CIOs in recognizing the key cybersecurity challenges and optimizing IT cost, risk and value to achieve their digital business outcomes.
Gartner projections show the growth in cybersecurity spend is slowing. Cybersecurity grew at 12% (CAGR) in 2018, and it is projected to decline to only 7% (CAGR) by 2023. Organizations are also reporting that after years of quarterly reporting on cybersecurity to their boards, they are now pushing back and asking for improved data and understanding of what they have achieved after years of such heavy investment.

Following Equifax’s hack in 2017, and their CEO consequently stepping down, it was reported that the CEO did not prioritize cybersecurity in the organization.¹

The severity of fines under the General Data Protection Regulation (GDPR) is based on the existence of adequate, reasonable, consistent and effective controls. This establishes a different type of standard to pursue appropriate levels of cybersecurity protection. The limitations of current approaches to security priorities, investment and governance are not in alignment with — or well-suited to address — this new standard. A better way to address this standard is to approach security as a business problem and align it with business needs. Organizations need to understand the limitations of their current execution and change their approach.

This research describes the limitations of many current organizational behaviors and approaches to cybersecurity, and establishes a foundation to pursue a new approach to cybersecurity measurement, reporting, priorities and investment.

Analysis

Address Failing Approaches to Cybersecurity

While cybersecurity has been on boards’ agendas, organizations face broad challenges to the effectiveness of cybersecurity, which must be addressed on priority (see Table 1).

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Societal perception of cybersecurity is that it is a technical problem, best handled by technical people.</td>
<td>Societal perception is dominated by fear, uncertainty and doubt. It results in poor engagement with peers, unproductive exchanges and unrealistic expectations. Ultimately, it leads to bad decisions and bad investments in cybersecurity.</td>
</tr>
<tr>
<td>Organizations are focused on the wrong questions about cybersecurity.</td>
<td>Unproductive questions are indicative of poor understanding, and drive attention away from an improved understanding and better investments.</td>
</tr>
</tbody>
</table>
1. Societal Perception Must Change to Avoid Bad Engagement and Investments

Current societal perception of cybersecurity can be characterized largely by fear, uncertainty and doubt, disconnected from the realities of addressing it. Society treats cybersecurity like a black box of technology.

Societal pressure has created guidance for boards that tells them to get smarter about cybersecurity and has driven governments to create regulations. While regulation forced organizations to act where nothing was being done, it has also created bad decision making in the context of checking boxes. While organizations believe that compliance will save them, the reality is that compliance does not equal protection. At worst, compliance forces organizations to spend money where they don’t need it and keeps them from investing where they should.

2. Organizations Are Asking the Wrong Questions About Cybersecurity

The most common questions related to cybersecurity governance asked by organizations establish a familiar pattern of demand emanating from executive leaders (see Table 2).

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current investments and approaches designed to address known limitations are not productive and are falling short.</td>
<td>Organizations are focused on new approaches that have great promise conceptually, but through a combination of failed execution and poorly set expectations, their investments are only delaying activities that will better improve cybersecurity.</td>
</tr>
<tr>
<td>Real failures are not getting enough attention to productively change behavior.</td>
<td>Compliance with any regulation does not equal appropriate levels of protection.</td>
</tr>
</tbody>
</table>

Source: Gartner (July 2020)

Table 2: Common Cybersecurity Questions and Their Limitations

<table>
<thead>
<tr>
<th>Question</th>
<th>Limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>How much should we spend on cybersecurity?</td>
<td>The amount an organization spends does not reflect its level of protection.</td>
</tr>
</tbody>
</table>
### Question

<table>
<thead>
<tr>
<th>Question</th>
<th>Limitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>How much does everyone else spend on cybersecurity?</td>
<td>The amount others spend does not inform the organization on its comparative protection with others’ level of protection.</td>
</tr>
<tr>
<td>What metrics should we report to the board?</td>
<td>The metrics most used today are trailing indicators of factors the organization does not control (i.e., how many times was the organization attacked last week?). The organization has to fix the underlying governance model before the metrics can be fixed.</td>
</tr>
<tr>
<td>How can we comply with regulation X?</td>
<td>Compliance with any regulation does not equal appropriate levels of protection.</td>
</tr>
<tr>
<td>How can we quantify cybersecurity risk?</td>
<td>Most representations of risk and security readiness in terms of money (i.e., is that a $5 million risk or a $50 million risk?) are not credible and defensible, and even when they are credible, they do not support daily decision making related to priorities and investments in security.</td>
</tr>
<tr>
<td>What tools should we implement?</td>
<td>Security capabilities are a function of people, process and technology. Leading with technology results in poor outcomes.</td>
</tr>
<tr>
<td>What are the most common threats in our industry?</td>
<td>Organizations do not control threats. They only control priorities and investments in security readiness.</td>
</tr>
<tr>
<td>How much security do we need?</td>
<td>This is a legitimate question, but every organization is seeking a simple answer where one does not exist.</td>
</tr>
</tbody>
</table>

Source: Gartner (July 2020)

These questions, and their answers, lead to bad decisions on priorities and investments in cybersecurity. At best, they lead to an approval for some version of the security budget. At worst, they lead to a false sense of security.

3. Rethink Cybersecurity Investments and Approaches That Fall Short
A number of organizational behaviors and investments drive cybersecurity to fall short. Executive leaders should ensure following behaviors and approaches are addressed to avoid cybersecurity failures:

a. The “Open-Checkbook” Abdication

Money alone does not solve cybersecurity problems. A major component of future cybersecurity success is the engagement of executive leaders. Money on cybersecurity must be spent in a business context. When executive leaders say they will provide all the money the CIO and/or CISO need to address cybersecurity, they are abdicating their role in oversight and participation in the process.

While this declaration is usually presented as a powerful show of support, unfortunately, this open checkbook makes it harder to engage executive leaders in a productive conversation to improve cybersecurity. An open checkbook puts the risk and responsibility completely on the CISO, instead of an organizational responsibility as a whole.

Access to budget is clearly important, but if that access comes at the expense of executive leaders’ engagement, it will harm the cybersecurity outcomes of the organization.

b. The Risk Appetite Failure to Execute

While developing risk appetite has great promise conceptually, in practice, it is falling severely short of the promise in most organizations.

A risk appetite is a representation of the business’s desire to accept risk. This is a modern concept and a reflection of the evolution from checklists to a risk-based approach. It is an important admission that risk is inevitable, and that risk is a tool that can be taken in measured doses to support business success. A clearly articulated risk appetite should give the organization an opportunity to express how much risk it is willing to take, and this can be used to guide cybersecurity investment in a business context.

The reality is that many risk appetite efforts have become platforms for the executive leaders to express zero tolerance for cybersecurity risk. The real failure of risk appetite efforts is the lack of a measurable scale of risk and an underlying governance process that enables effective risk decision making. Lacking these basic components drives risk appetite statements to fall short of its promise and, eventually, become abandoned.

c. Quantification Being Treated as a Panacea

Quantification has been growing in interest within organizations, fueled by needs to present risk and security in terms of money and likelihood of damage. It has reached a near-fever pitch of inflated expectations in 2020. However, there are several observations that indicate it will not materially impact most organizations. Every organization must match its interest in quantification against the below considerations to determine if it is right for the organization:
1. Quantification takes significant resources in time, money and full-time equivalent (FTE) person/labor hours to develop credible and defensible results. Smaller organizations will struggle to have sufficient data for their organizations to create credible and defensible results and will lack the resources to execute.

2. Organizations must beware of quantification misuse. Several organizations have engaged in quantification exercises that produce exactly what they need as far as charts, evidence of rigor and quantified results are concerned. The problem is that down inside their calculations sit assumptions and “expert opinion” that essentially dictate the result. Executive leaders should ensure peers made accountable for quantification have detailed understanding of the organizational risk requirements to fully support improved cybersecurity.

3. Organizations should assess the value of the results in supporting improved decision making. As part of an evaluation, executive leaders should ask their peers to explore a thought exercise related to how the results would be used. Quantification shows value in supporting how much cyberinsurance an organization needs, for example. But it does not support daily investment decisions that every organization needs to make related to priorities and investments in cybersecurity.

d. Internal Audit and Regulatory Compliance Remain as Primary Drivers

Many boards still believe that internal audit and regulatory compliance are their primary guides to address cybersecurity. There are several indicators of this, including:

- Cybersecurity board reporting buried in the audit committee
- A focus on addressing internal audit findings over building an effective program
- The number of organizations where cybersecurity reports into an organization called “audit and compliance” or “risk and compliance”
- The checkbox mentality is still a material mindset in many organizations

Compliance does not equal protection and internal auditors should not dictate how much risk is acceptable or which controls are most important. Checkboxes create spend in areas where organizations don’t need it and take resources away from areas where they do.

4. Discuss Real Failures Caused by the Disconnect Between Cybersecurity and Business Decision Making

Gartner’s analysis of Equifax’s 2017 cybersecurity breach, and the consequent congressional testimony of its CEO, revealed a disconnect between executive understanding and levels of cybersecurity capabilities in the organization.

These disconnects should create a wake-up call for executive leaders and their peers to the critical need to address cybersecurity in a business context and as a business decision. They should use
the following examples in a board narrative to illuminate the risk of cybersecurity to business outcomes beyond hackers and data breaches:

**Example 1: Inconsiderate engagement of risk.** A decision maker at a bank chose to ignore a risk assessment recommendation for multifactor authentication on a new customer-facing online banking application. This decision maker had the authority to shut it down, and ironically, it may have been the right business decision to protect customer experience. The failure is that this decision maker had no understanding or accountability for the security of the application.

**Example 2: Engineering failure in a cyber-physical system.** A field engineer gathered configuration telemetry from a large field installation across several acres of large moving machines, and fed the information into a simulation program back at the manufacturer’s headquarters. Due to a misconfiguration, the program risked millions of dollars in damage and human safety due to lack of consideration of security in the product management process.

**Example 3: Cybersecurity as an existential threat.** The manufacturer of a device for shop floors globally had ignored cybersecurity in the development of its internet-connected product. The foundation software was open source and riddled with vulnerabilities. The dark web identified all of its devices connected to the internet and the company became host for every imaginable cybercrime, from money laundering to distributed denial-of-service bot controllers. Its executives were notified, but did not care, because none of their shop floor customers complained. This is a business waiting to be sued out of existence for liability.

**Example 4: Lack of decision makers’ understanding related to third-party risk.** A financial services organization, with full support of the board, decided to pursue a business strategy of outsourcing many of its business functions. The security team established a rigorous assessment process to inform business decision makers about security risks and to make go/no-go recommendations on working with certain partners. A business decision was made to engage one particular partner, despite a material recommendation to not engage that firm due to security weaknesses. Six months into the engagement, the company suffered a material breach for the same control weaknesses that were raised in the recommendation. The board held the security officer responsible for the failure. Follow-ups with the board focused on improving the board’s understanding of third-party risk and emphasizing the impact of business unit decision making on material security posture.

These examples show that business decision making disconnected from the realities of business impact can lead to serious business harm.

Broken governance is a business decision that impacts cybersecurity readiness, but is made with no consideration of that impact. There is little or no accountability and little evidence that the risks are described appropriately in a business context. So, executive leaders often don’t understand the risk they are signing off on.
This disconnect between executive decision making and effective cybersecurity is what should focus executive leaders’ attention on new ways to approach the problem. The first critical step is to create a business context around cybersecurity.

Create a Business Context Around Cybersecurity

Every organization has budgets and costs, desired business outcomes and supporting business processes, sources of revenue and customers. And they all have technology dependencies. These dependencies create a need for investment to protect the technologies that support organizational business outcomes. Understanding an organization's most important business outcomes, processes and technology outcomes is the first step in putting a business context around cybersecurity.

The Limitations of Current Standards, Frameworks and Maturity Models for Cybersecurity

Cybersecurity standards and frameworks are published recommendations to secure an environment. The principal objective of these standards is to reduce cybersecurity risks. They generally include collections of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best-practice assurance and technologies.

Process maturity models use the guidance in the standards and frameworks to extract best practices and techniques in determining capability levels. Together, they guide priorities and investments to achieve desired levels of cybersecurity capability. Their biggest limitation is that maturity models measure how good capabilities are, not what they are achieving. Moreover, as organizations achieve higher maturity, these maturity models, frameworks and standards begin to lose their value.

Regulators have also signaled that cybersecurity capabilities must have characteristics beyond those commonly represented and audited in maturity models and existing standards. Organizations need something more powerful that has a direct line of sight to the delivered levels of protection.

Adopt Outcome-Driven Metrics for Cybersecurity

An assessment of an audit standard for the National Institute of Standards and Technology (NIST) Cybersecurity Framework showed that 73% of the audit questions are related to the existence of controls, not their performance or levels of protection.²

Outcome-driven metrics (ODM) for technology risk are an abstraction of tools, people and processes to reflect how well an organization is protected, not how it is protected. ODM can be used to enable more effective governance over cybersecurity priorities and investments. It creates the language necessary to have meaningful business-focused conversations with executives and boards. Executive leaders should ensure ODMs are leveraged to drive more business-focused cybersecurity discussions in their organizations.
A Standard for Effective Cybersecurity Readiness and Investment

According to Elizabeth Denham, the U.K. Information Commissioner, the severity of GDPR fines following major cybersecurity breaches is not related to organizations getting hacked or the number of people impacted; rather, it is related to the presence of adequate, reasonable, consistent and effective controls. This clarification offers the opportunity to define a new standard based on a new way to approach appropriate levels of protection, called the CARE (consistent, adequate, reasonable and effective) standard for cybersecurity (see Figure 1).

**Figure 1: The CARE Standard for Cybersecurity**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td><strong>Consistent</strong>: Do your controls work the same way over time?</td>
</tr>
<tr>
<td>A</td>
<td><strong>Adequate</strong>: Do you have satisfactory and acceptable controls in line with business need?</td>
</tr>
<tr>
<td>R</td>
<td><strong>Reasonable</strong>: Do you have appropriate, fair and moderate controls?</td>
</tr>
<tr>
<td>E</td>
<td><strong>Effective</strong>: Are your controls successful in producing the desired or intended results?</td>
</tr>
</tbody>
</table>

Ultimately, these are value judgements that must be credible and defensible. It supports the creation of a balance between protection and running the business. It also embodies the incentive to build a better security capability that delivers better outcomes, not just spend more money on security.

**Cybersecurity Readiness Is a Choice**

The purpose of a security program is not to protect the organization, because that is an impossible goal. In a modern security program, the purpose is to balance the need to protect with the need to run the business.

Cybersecurity readiness is a choice. Executive leaders should work with their peers and direct reports to enable the creation of adequate, reasonable, consistent and effective controls that are credible and defensible with their key stakeholders, i.e., shareholders, regulators and customers.

The urgency to treat cybersecurity as a business decision has never been greater. Organizations now have the understanding and guidance to reinforce their cybersecurity strategies.

**Evidence**

1. “8 Reasons More CEOs Will Be Fired Over Cybersecurity Incidents”

2. “Outcome-Driven Metrics for Cybersecurity in the Digital Era”

Recommended by the Author

A Decision Model to Optimize Risk, Value and Cost
The CARE Standard for Cybersecurity
Optimize Risk, Value and Cost in Cybersecurity and Technology Risk
Outcome-Driven Metrics for Cybersecurity in the Digital Era
An Outcome-Driven Approach to Cybersecurity Improves Executive Decision Making

Recommended For You

Best Practices for Creating an Enterprise Information Security Charter
Toolkit: Sample Information Security Administrator Job Description
Five Things Leaders Can Do Today to be More Inclusive
Implementing Aligned Assurance Part 1: Laying the Foundation for Aligned Assurance
Managing Strategic Talent Risk

© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner’s prior written permission. It consists of the opinions of Gartner’s research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner’s Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."