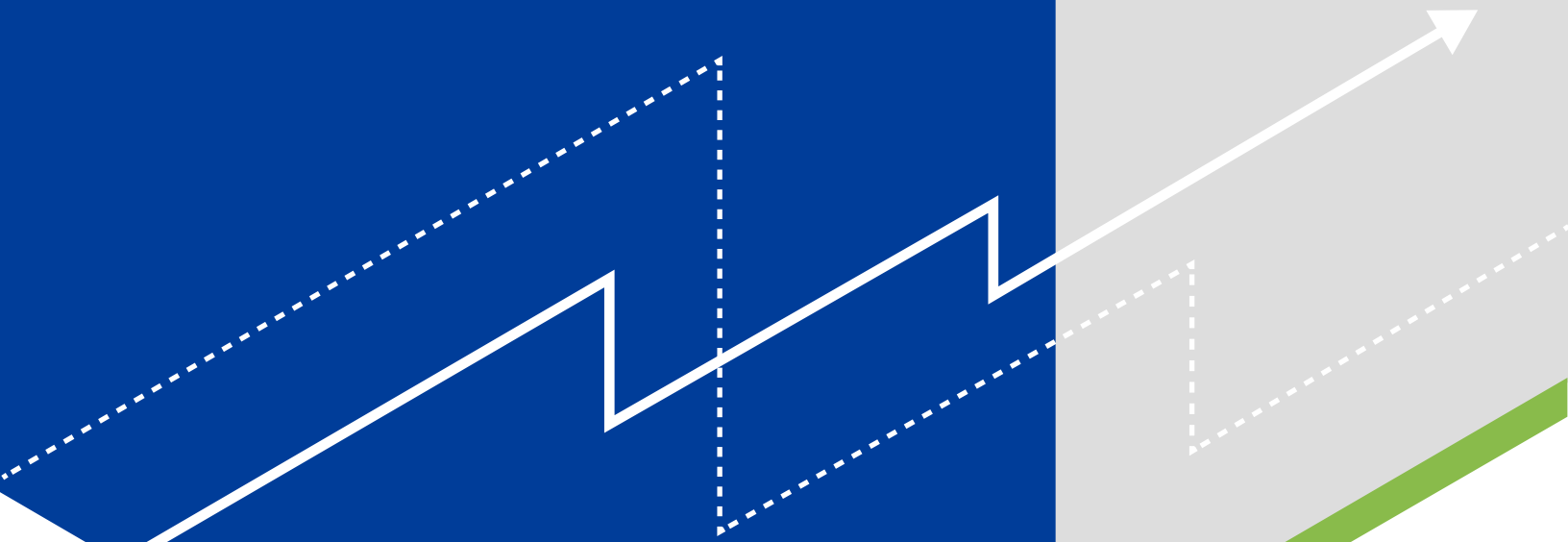
A Forrester Consulting
Thought Leadership Paper
Commissioned By BitSight

September 2019

Better Security And Business Outcomes With Security Performance Management

Mitigating Risk And Generating Revenue With Metrics That Matter



FORRESTER®

Table Of Contents

Project Director:
Emma Van Pelt,
Market Impact Consultant

Contributing Research:
Forrester's Security & Risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Calls from customers and partners for security transparency are increasing. The heat is on CISOs, CROs, and CIOs to report on the metrics that truly measure the effectiveness of security. Only then can they understand the business impact of their security programs.

Executive Summary

In today's competitive marketplace, security has become a crucial market differentiator. Companies increasingly realize that security is critical to: earning customer trust; securing intellectual property; and protecting the brand. Customers want to do business with secure businesses — and since empowered customers can easily move their business elsewhere if they feel vulnerable, security decision makers must understand and measure their program's effectiveness and communicate that to internal and external stakeholders. They must be on the lookout for indications of failure that will most harm the business. In short, security needs metrics that matter.[1]

The pressure is on chief information security officers (CISOs) to, first and foremost, create an effective security program. They then must capture metrics that accurately and objectively measure the program, in order to meet the demands of both customers, for transparent reporting, and boards of directors, for efficient investments — a discipline known as security performance management (SPM). While security has traditionally been reactive in nature, with its metrics focused on minimizing costs through breach avoidance, SPM provides the opportunity to define security more strategically, with proactive and risk-based performance metrics.[2] Though many security organizations seek effective SPM, organizational misalignment and technological complexity have been challenging to overcome.

BitSight commissioned Forrester Consulting to evaluate how security leaders measure their enterprise's security performance. Forrester conducted an online survey with 207 security decision makers with responsibility for risk, compliance, and/or communications with boards of directors to explore this topic. We found that C-level leaders are struggling to understand how their security is performing and how to adequately report that performance to the board and other C-level leadership.

KEY FINDINGS

- **Company reputation and the ability to attract new business is at risk because of security.** Companies agree that C-level security leaders are stewards of company reputation and that customer demands for cybersecurity reporting have intensified in recent years. The inability to measure or communicate security performance to customers, regulators, and executives puts businesses at risk.
- **Improved security measurement would greatly improve company financial performance and reduce risk.** Nearly three-quarters of C-level respondents say that improved security performance measurement would greatly or significantly improve company financial performance. More than half of companies overall say improving measurement would reduce overall risk.
- **Improved security measurement helps security professionals build effective business cases, resulting in expanded budget.** Metrics make for strong, persuasive business cases; companies that have implemented formal security performance metrics are more likely to have seen a 10% or greater increase in security budget year over year.

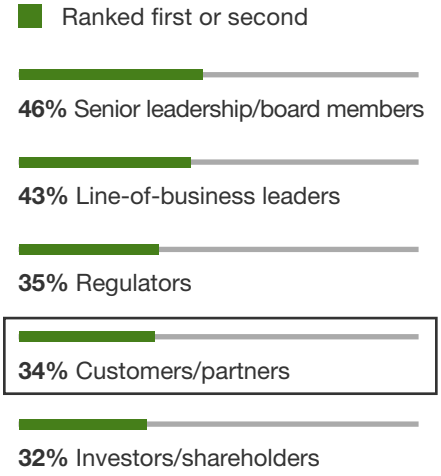
CISOs: It's Time To Manage Security Like A Business

Companies win and lose business based on both real and perceived security performance challenges — meaning security is now responsible for protecting, enabling, and even creating, revenue growth opportunities. This stems from the simple fact that customers are more willing to do business with companies that have good security, as they know their data and intellectual property are protected.[3] The power that security has to drive revenue has thrust many CIOs, CROs, and CISOs into a new spotlight; for leaders that traditionally hail from technology, rather than from business management backgrounds, the evolution of their role can be uncomfortable. To help these leaders better understand their new responsibilities, our study of 207 security decision makers illustrates the forces that shape the new security-business paradigm:

- **Customers and partners have priority.** We found that 80% of companies we surveyed experienced a cybersecurity incident in the past year, the most common being malware attacks. These security incidents affect customer privacy/safety the most — 54% report customers were greatly or somewhat harmed by an incident. Since customers are more likely to do business with companies with good security, both demonstrating and communicating security efforts have never been more critical. In fact, 79% of companies agree that customer/partner demands for cybersecurity reporting have intensified in recent years. However, our findings revealed that customers and partners receive some of the least accurate reporting — less accurate than board members, line-of-business leaders, and regulators (see Figure 1). It would seem that although effective communication with customers and partners should be the priority, security leaders aren't properly addressing their demands.
- **Reputation is integral to business success.** Customer perception means real money: More than one-third of companies agree that they have lost business due to either a real or perceived lack of security rigor (see Figure 2). Additionally, 82% of decision makers agree that the way customers and partners perceive security is increasingly important to the way their firm makes decisions. The growing importance of reputation has made it so the opinions and perceptions of customers and partners now have a greater bearing on security decisions than those of regulators. Where regulatory compliance may have once been the deciding factor in security decisions, companies have begun prioritizing the perspectives of their customers and partners — likely because they directly determine the ability to do future business.

Figure 1

"For which audience do you feel you best provide metrics that accurately measure your security performance?"



Base: 207 US & UK risk, compliance, & security decision makers who are responsible for overseeing communications with the board of directors
Source: A commissioned study conducted by Forrester Consulting on behalf of BitSight, May 2019

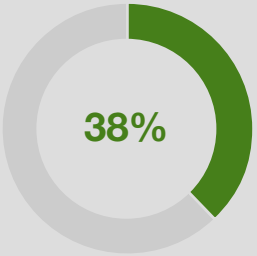
› **CISOs are responsible for communicating security's effectiveness to key audiences.** Security is evolving into a business discipline, but this isn't dawning on everyone in the security ranks equally. We found that, in the wake of an incident, C-level security decision makers are more likely than their staff to cite harm to company reputation and customer acquisition— meaning that C-level decision makers understand the value of effective security better than their direct reports (see Figure 3). As the discipline matures, CISOs will play the role of translator for their organization: explaining up to the CEO what they are doing to secure the business' ability to generate more revenue, as well as explaining down to direct reports on why it's important to set security goals aligned to business objectives.[4]

Companies can no longer simply share results of a successful audit to prove they have good security performance. CISOs understand that while their audits are important boxes to check, security outcomes are what really matter to customers. Security leaders need to capture, track, and report on security metrics that truly measure security effectiveness, built on meaningful measurement that all stakeholders can understand.

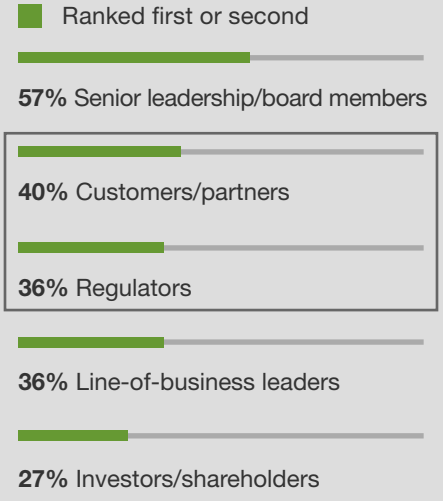
Figure 2

Companies Lose Business Based On Real Or Perceived Security Issues; Customer Opinion Outranks Regulators In Security Decisions

"We have lost business due to a perceived or real lack of security rigor."



"Which audience's perceptions/opinions regarding security have the greatest bearing on how your organization makes security decisions today?"



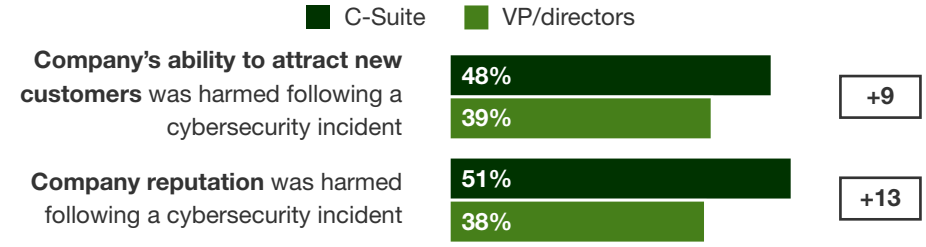
Base: 207 US & UK risk, compliance, & security decision makers who are responsible for overseeing communications with the board of directors
Source: A commissioned study conducted by Forrester Consulting on behalf of BitSight, May 2019

The opinions of customers and partners have begun to shape the cybersecurity decisions that companies make.

FORRESTER®

Figure 3

C-levels Understand They Sacrifice Business When Security Fails



Base: 102 C-levels; 64 VP/directors; US & UK for risk, compliance, & security for overseeing communications with board of directors who experienced a security incident in the past year
Source: A commissioned study conducted by Forrester Consulting on behalf of BitSight, May 2019

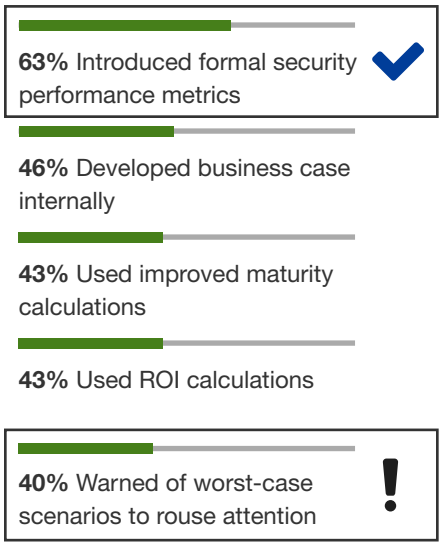
You Can't Manage What You Can't Measure

CISOs must begin to manage their department through a business-focused lens. They are increasingly on the hook to answer questions like: How does security align with and support overall business objectives? What goals should be set? And how should we measure and report on progress toward those goals? Our survey uncovered that security leaders need metrics to understand performance and provide assurance to customers and partners beyond an audit in order to enable business growth. But current SPM practices only scratch the surface of what's possible:

- **Security metrics are becoming critical to planning budgets, but the maturity of managing security as a business is still low.** Security is evolving into a business discipline. There is increased scrutiny on spending (70% agree), and formal metrics are now the key method to justify investments (an approach at 63% of companies). However, 63% is still low considering how important measurement is. And it's also important to note that 40% say they have warned decision makers of worst-case scenarios to rouse attention in order to justify investments — a far cry from a precise business case (see Figure 4).
- **Cybersecurity risk ratings emerge as an early security measurement bright spot.** Even though SPM is in its early stages, we discovered one encouraging trend: 45% of companies use cybersecurity ratings, making it the third most common metric overall (see Figure 5). These independent security ratings are a measurement of an organization's security performance derived from objective, verifiable information and created by an independent organization. Since they are risk-focused, they are more strategic by nature than other common security metrics. However, the value of ratings appears to extend further than that. We found that 43% of companies using cybersecurity ratings also report them out to customers and partners, more so than any other metric. It's intriguing that cybersecurity ratings have an early advantage in security performance reporting to customers — something increasingly critical to winning business.

Figure 4

"Which of the following approaches have you used to help justify current or proposed security investments?"
Top five approaches shown



Base: 207 US & UK risk, compliance, & security decision makers who are responsible for overseeing communications with the board of directors
Source: A commissioned study conducted by Forrester Consulting on behalf of BitSight, May 2019

FORRESTER®

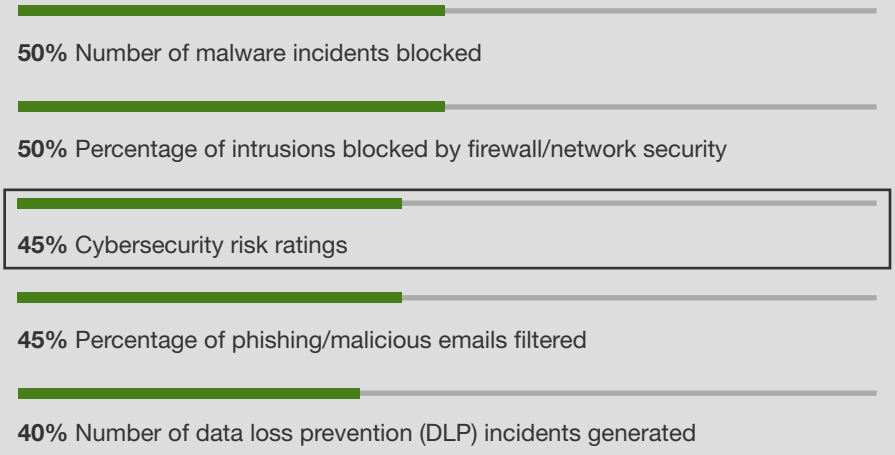
› **Other common security metrics tell an incomplete story.** Our study found that the other four of the top five security metrics used today are flawed in several ways (again, see Figure 5). Metrics like the number of malware incidents blocked or number of data loss prevention incidents generated are not contextualized figures (i.e., a company may count that the firewall blocked 1 million intrusions, but it doesn't report how many they let in). Other metrics in the top five, like the percentage of intrusions blocked by firewalls or the percentage of phishing emails filtered, may provide greater context (by reporting as a percentage). But, they can also miss the mark in other troubling ways, including: 1) only reporting on the limited scope of what existing instrumentation measures, leading to potential blind spots, and 2) highlighting information based on queries that only reflect the analytical skills of the architect, leading to bias.[5] Traditional metrics paint an incomplete picture and can leave companies blind to potential risk.

› **The board sees metrics that don't fully measure security's effectiveness.** The intended audience for security metrics further highlights the CISO's challenge to be an effective security translator within the organization. For example, we found that 63% of firms that measure the number of blocked malware incidents also report the metric up to the board. But because this metric provides no larger context and is subject to analytical bias, it is inappropriate for strategic board-level discussions. Metrics like this don't meaningfully communicate exposure or performance to executives, regulators, business partners, or customers. However, one encouraging point of comparison is that 63% of companies using cybersecurity ratings also report them up to the board, and since these ratings are more risk-focused, objective, and outcome-based, they are appropriate for board-level discussions.

Figure 5

Companies Don't Fully Measure How Security Performance Affects Their Business

"How do you measure security performance today?" Top five metrics shown



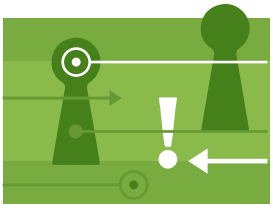
One encouraging caveat: 45% use cybersecurity risk ratings. Since these are risk-focused, they are more strategic than the other common metrics today.

Base: 207 US & UK risk, compliance, & security decision makers who are responsible for overseeing communications with the board of directors
Source: A commissioned study conducted by Forrester Consulting on behalf of BitSight, May 2019

FORRESTER®

› **In the absence of meaningful metrics, companies amass more data — even though they struggle to analyze it as it grows.** In an effort to gather more data on their performance, companies have invested in new technology as a way to improve security performance measurement (63%). This isn't surprising given the technology background of most security leaders; technologists tend to seek out technology. But technology adoption has led to an increasingly complex security ecosystem (we found that companies have an average of nine different categories of security technologies in place) — and more data gathered by these tools doesn't necessarily mean better decisions. In fact, we found that analyzing data from security tools and technologies is the top challenge to measuring security performance. Without meaningful metrics in place to measure effectiveness and communicate value, companies are left awash in data they are unable to contextualize.

Improved performance metrics would allow companies to judge data's significance, make better decisions, and provide a foundation for more secure, and therefore, more fruitful customer relationships. Security decision makers will have to do more than collect data if they are to succeed in running their programs as a business.



Analyzing data from a growing number of tools is the top challenge in measuring security performance. CISOs need effective metrics in place to put their valuable data in context and improve security outcomes.

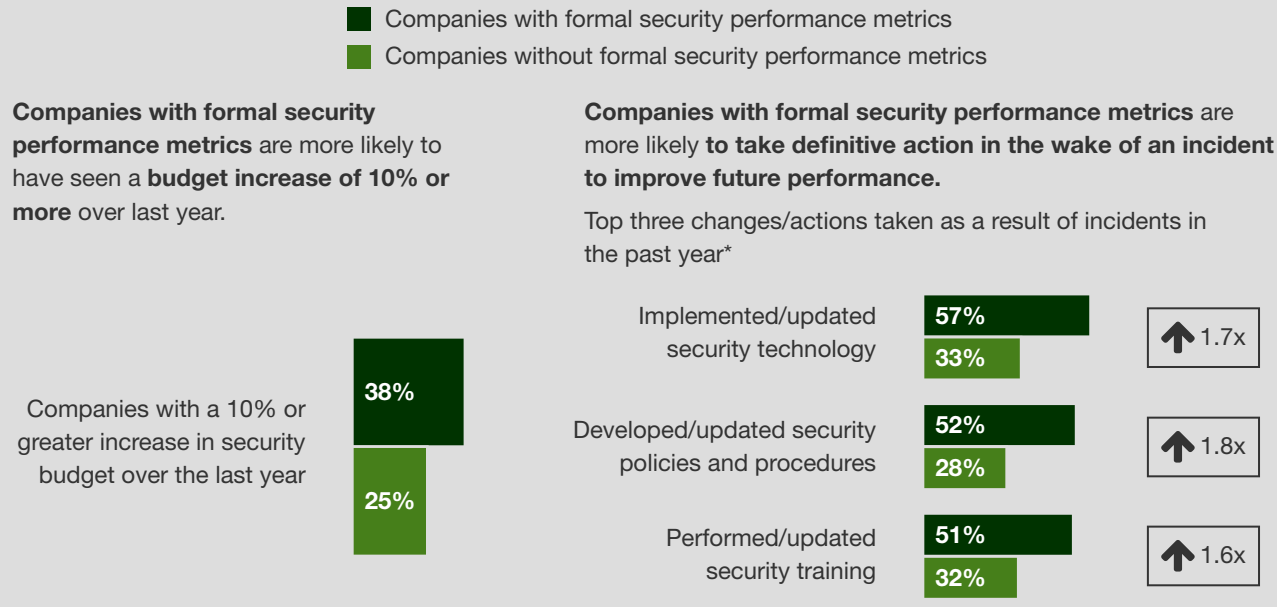
The Path To Security Performance Management

Companies need to adopt SPM in order to increase security effectiveness and meet the demands for transparent reporting. Our study found that companies in the early stages of SPM are now even experiencing wins. Companies tracking formal security metrics are more likely to:

- **Increase security budget.** Companies using formal security metrics are more likely to have seen a 10% or greater increase in their security budget over last year (38% of firms with formal metrics said this versus just 25% of firms without formal metrics) (see Figure 6).
- **Improve program effectiveness.** It's not just about budget: companies that formally monitor, measure, and track performance are better at managing security outcomes — we know this because companies with formal metrics are 1.8x more likely to develop security policies, 1.7x more likely to update security technology, and 1.6x more likely to perform security training (again, see Figure 6). Taken together, companies that track performance can better justify their security budget and are more likely to take action to improve security outcomes.

Figure 6

Companies With Formal Security Performance Metrics Are Reaping Benefits



Base: 130 implemented, 77 not implemented US & UK risk, compliance, & security decision makers who are responsible for overseeing communications with the board of directors
*Base: 109 implemented, 57 not implemented US & UK risk, compliance, & security decision makers who are responsible for overseeing communications with the board of directors who experienced an incident in the past year
Source: A commissioned study conducted by Forrester Consulting on behalf of BitSight, May 2019

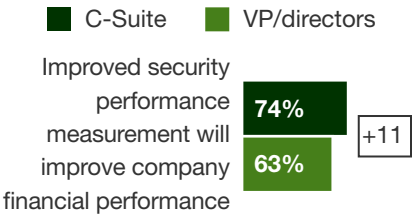
FORRESTER®

Given the clear benefits their peers experience, it should come as no surprise that companies overall believe that by improving security performance measurement, they can:

- **Improve financial performance.** Nearly three-quarters of C-level respondents said that improved security performance measurement would greatly or significantly improve company financial performance (see Figure 7). Companies in our survey also reported that improved measurement would improve company business continuity (82%) and company reputation (81%) — direct indicators of the business's ability to take in and grow revenue (see Figure 8).
- **Increase customer value.** Companies agree improved security performance measurement creates value by improving outcomes in the areas that closely touch their customers' lives: preventing and detecting breaches (again, see Figure 8). More broadly, over half of companies associate better security performance measurement with reduced risk overall.

Figure 7

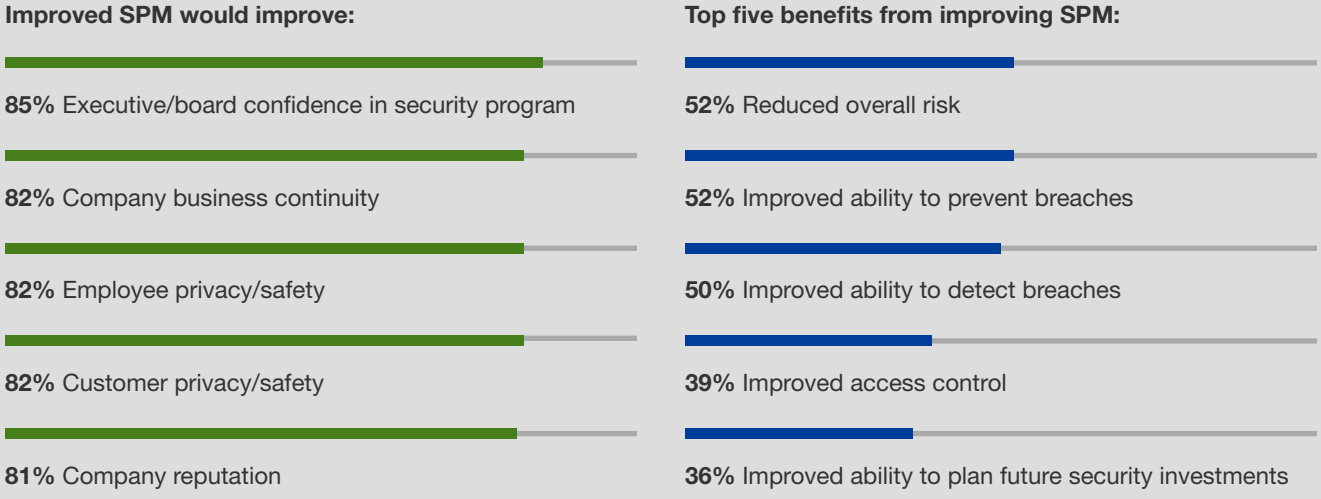
CISOs Believe SPM Leads To Improved Financial Performance



Base: 121 C-levels; 86 VP/Directors; US & UK for risk, compliance & security, responsible for overseeing communications with board of directors
Source: A commissioned study conducted by Forrester Consulting on behalf of BitSight, May 2019

Figure 8

Security Leaders Believe Improved SPM Will Improve Business And Security Outcomes Simultaneously



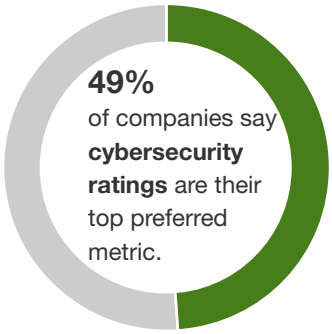
Base: 207 US & UK risk, compliance, & security decision makers who are responsible for overseeing communications with the board of directors
Source: A commissioned study conducted by Forrester Consulting on behalf of BitSight, May 2019

FORRESTER®

LEVELING UP: LOOKING AHEAD TO ADVANCED SECURITY PERFORMANCE METRICS

So far, our discussion has focused on how metrics help companies measure performance so that security leaders can report up and out on effectiveness and win more business. However, our study revealed that some companies are interested in taking on advanced performance metrics — metrics that go a step further by more directly measuring the strategic, operational, and tactical elements of security's relationship to business outcomes. Though many of these metrics are considered aspirational today, they are potent examples for how companies can approach security measurement from different angles:

- **Strategic metrics** that show the current and potential business impact of security risks and the efforts to mitigate them; information that might affect brand, reputation, or other factors linked to revenue. For example:
  - The percentage of critical business systems meeting security SLAs is a strategic metric that targets security efficacy.
  - The retention rates of employees with access to intellectual property is a strategic metric for risk associated with employee turnover.
- **Operational metrics** that provide an overview of performance and interrelationships across the organization; information that can lead to adjustments in the allocation of team resources and the direction of projects and initiatives. For example:
  - The number of high-value financial transactions blocked by security is an operational metric for security's business enablement.
  - The average number of days to fill open security positions is an operational metric for the performance of security staffing efforts.
- **Tactical metrics** that apply to staff who directly control technologies and processes across security workflows; information that helps security analysts and frontline employees make better decisions. For example:
  - The number of currently open customer security issues is a tactical metric for performance of customer support.
  - The number of reported breaches among peer organizations is a tactical metric for industry incident vulnerability.[6]



Cybersecurity ratings are the No. 1 preferred metric (49%). Because they are a strategic, risk-focused metric, it's encouraging to see them those ratings rise to the top.

Companies interested in advanced metrics stand out in both their understanding of what's at stake for their company and the actions they already take to improve outcomes (see Figure 9 for more examples of advanced metrics). We found:

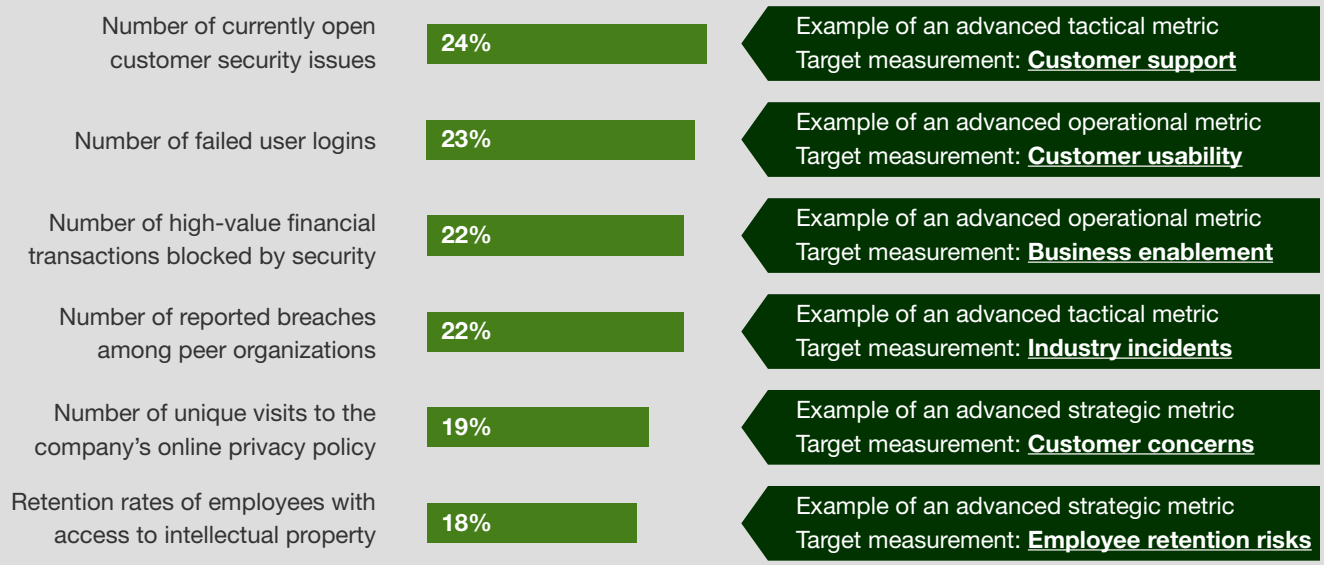
› **Mature companies seek improved performance metrics.** Looking more closely at companies with interest in two or more advanced metrics, we find they look different than other companies in three key ways: 1) they are more likely to understand that business is at stake when security fails; 2) they are more confident in their ability to provide accurate reporting to customers/partners; and 3) they are less likely to over-rely on new technology adoption and more likely to work cross-functionally to centralize data (see Figure 10). Taken together, these firms better understand security's ability to enable business growth and are taking proactive steps to improve their security performance.

› **C-level execs understand what's at stake and now need to lead.** Given their especially strong awareness of the business' need for improved reporting, C-level security respondents are more likely to list advanced metrics as ideal. Take the metric "number of failed user log-ins," for example. This measures the number of customers trying to log-in but failing because they don't know their password, they forget the answers to their preset security questions, etc. It's considered an advanced metric because it is a leading indicator of security's effect on customer usability and therefore captures a potential business risk if customers are unable to easily gain access to the services they want.[7] For this metric, 27% of C-level respondents put it in their top five preferred metrics versus only 17% of VPs and directors.

Improved security performance measurement is a tremendous opportunity for security leaders who want to better align with the business. C-level leaders believe security can contribute to the organization's goals and now they need to step up to provide meaningful metrics.

Figure 9

"Of the metrics below, which would you most wish to use to measure security performance?"



Base: 207 US & UK risk, compliance, & security decision makers who are responsible for overseeing communications with the board of directors
Source: A commissioned study conducted by Forrester Consulting on behalf of BitSight, May 2019

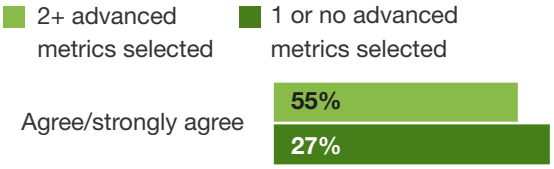
FORRESTER®

Figure 10

Companies Seeking Advanced Metrics Are More Mature

These companies are more likely to understand **lost business opportunities connected to security reputation.**

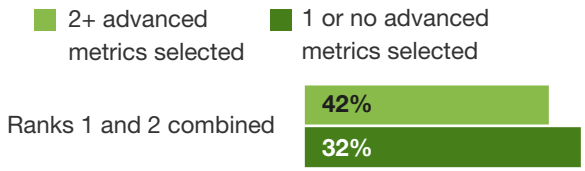
"We have lost business due to either a perceived or genuine lack of security rigor."

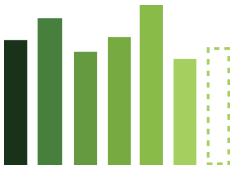


These companies are better **at proving diligence to customers and partners.**

"For which audience do you feel you best provide metrics today?"

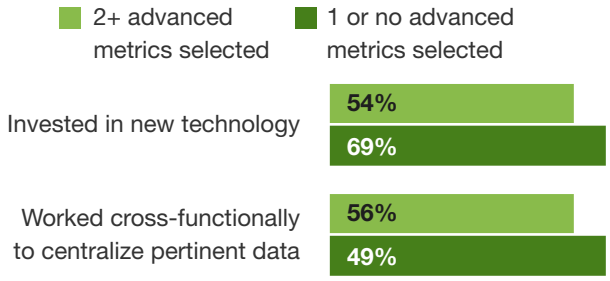
Customers/partners





These companies are better at **aligning across the business to improve security performance.**

"What steps have you taken, if any, to improve security performance measurement?"

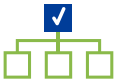


Base: 81 2+ advanced metrics, 126 1 or no advanced metrics; US & UK risk, compliance, & security decision makers who are responsible for overseeing communications with the board of directors
Source: A commissioned study conducted by Forrester Consulting on behalf of BitSight, May 2019

Key Recommendations

Security performance measurement helps you articulate the effectiveness of your program to your business stakeholders, which helps demonstrate security's overall value. However, not all security metrics are made equally, and getting to the point where you can accurately measure and communicate security risk to your business is no easy task.

Forrester's in-depth survey of 207 security decision makers about security performance measurement yielded several important recommendations:



Seize the opportunity while senior executives focus on cybersecurity. Cybersecurity is now a board-level topic and one that senior business stakeholders believe contributes to the financial performance of their firm. Develop meaningful security metrics that highlight how an effective security program helps preserve and protect brand and reputation to avoid squandering the spotlight.

Build security's brand by measuring security performance. For security leaders seeking to increase their credibility with senior business leaders and their firm's board of directors, there is no better way to improve confidence in cybersecurity than with a set of mature, SPM metrics.

Leverage metrics to combat the data deluge and make better decisions for your business. When it comes to establishing meaningful metrics, security leaders are often their own worst enemy. The instinct to solve security problems with technology results in a complex technology ecosystem with a growing amount of disjointed data and no way to analyze it. Risk-based metrics help you understand where and how you need to prioritize investments in your security program. In addition to immediate decisions, they help you plan for future decisions, as well as view the results of prior decisions.

Keep metrics focused on customers, partners, and business performance. Align your program metrics to your business metrics to understand how your business creates value for customers. Connect your metrics to the relevant customer-facing employees, data, applications, systems, and processes. Mature metrics connected to your business will make the effectiveness of your security program clear when you share your metrics with customers, partners, and other non-security colleagues.

Appendix A: Methodology

In this study, Forrester interviewed an online survey of 207 organizations across industries in the US and the UK to evaluate security performance measurement. Survey participants included decision makers in IT, security, risk, and compliance. Questions provided to the participants asked how they measure security performance, how they are performing, and how they are planning to improve measurement. Respondents were offered a small monetary incentive as a thank you for time spent on the survey. The study began in February 2019 and was completed in May 2019.

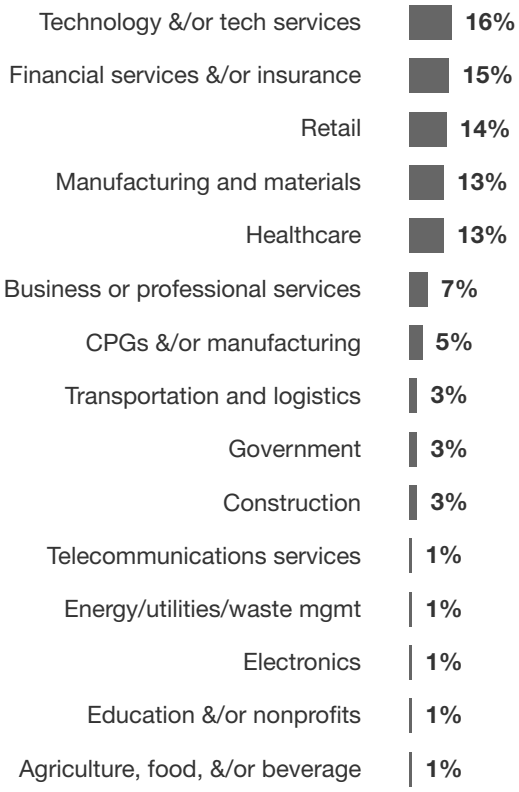
Appendix B: Demographics/Data

COUNTRY

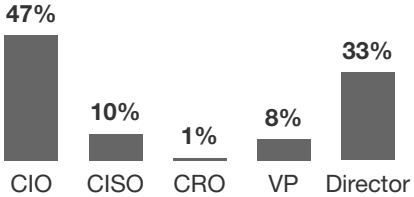
50% US

50% UK

INDUSTRY



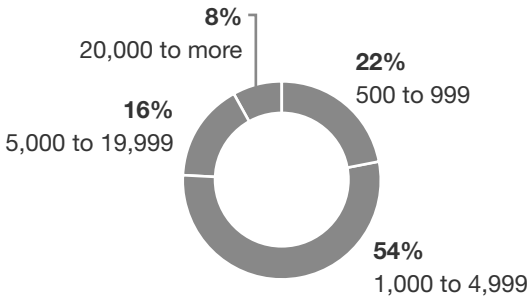
TITLE



DEPARTMENT

92% IT
5% Cybersecurity
3% Risk & compliance

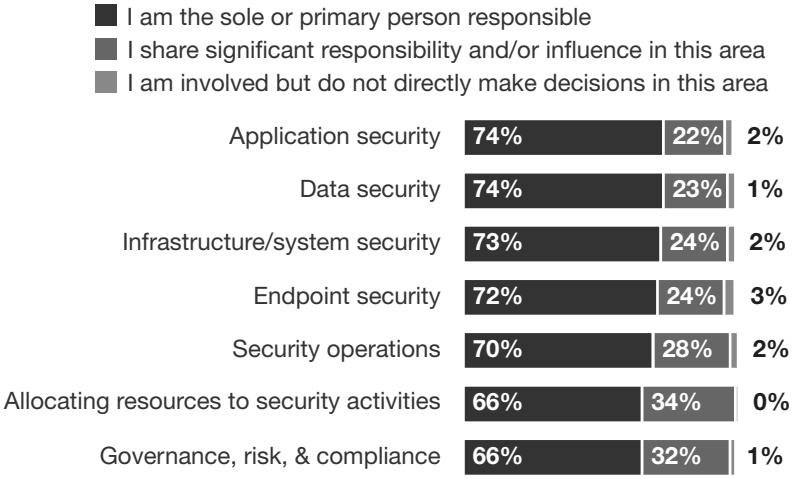
NUMBER OF EMPLOYEES



Responsibility for measuring, reporting, decision making regarding security performance

82% Primary responsible
16% Share primary responsibility
2% Contributor

RESPONSIBILITY AREAS



Base: 207 US & UK risk, compliance, & security decision makers who are responsible for overseeing communications with the board of directors
Source: A commissioned study conducted by Forrester Consulting on behalf of BitSight, May 2019

FORRESTER®

Appendix C: Supplemental Material

RELATED FORRESTER RESEARCH

"Security For Profit," Forrester Research, Inc., March 14, 2019.

"Remove The Mystery From Security Metrics," Forrester Research, Inc., November 16, 2018.

Appendix D: Endnotes

[1] Source: "Security For Profit," Forrester Research, Inc., March 14, 2019.

[2] Source: Ibid.

[3] Source: Ibid.

[4] Source: "Remove The Mystery From Security Metrics," Forrester Research, Inc., November 16, 2018.

[5] Source: Ibid.

[6] Read the complete guide to metrics that CISOs can use to steer the security team's efforts, allocate resources strategically, and communicate results with stakeholders throughout the organization. See the Forrester report "Remove The Mystery From Security Metrics [45787]."

[7] Source: Ibid.