FORRESTER®

Forrester Opportunity Snapshot: A Custom Study Commissioned By Agile 3, An IBM Company | January 2018

Is Your Company In Peril If Critical Data Is Breached?

How Executive-Level Security Tools Can Protect Your Business

GET STARTED ▶

Forrester Opportunity Snapshot: A Custom Study Commissioned By Agile 3, An IBM Company | January 2018

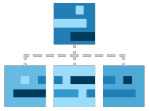
Is Your Company In Peril If Critical Data Is Breached?

Overview

Critical data and information — including customer data, intellectual property, and strategic plans — are key to organizations' competitiveness, but a breach of this data can have disastrous consequences. Though data security has long been the purview of IT and security teams, the market is shifting, and business executives must take notice. Our study found that CEOs and the board of directors (BoD) are the most accountable to external stakeholders when data is compromised. As evidenced by recent, highly publicized executive departures following a breach, their jobs are literally at risk. Other disastrous consequences include incident response costs, General Data Protection Regulation (GDPR) fines, plummeting stock prices, and shattered reputations. One thing is clear: A data risk management program is critical.

Business leaders must play an active role in protecting against the risks associated with breaches of critical business data and intellectual property. But IT, security, and risk teams speak a different language from the business leaders and struggle to equip them with the information they need to make effective decisions. Tools that give executives business-relevant data security visibility can help bridge the divide.

In September 2017, Agile 3, an IBM company, commissioned Forrester Consulting to survey 150 IT, security, and risk decision makers and examine their approach to protecting their company's critical data and information and communicating data risk to senior business executives.

51% 

believe the CEO or the BoD is most accountable to external parties following a data breach.

58%

have suffered from a breach of critical data recently; among the rest, three out of five admit they're uncertain if they've been affected.

65%

of IT and security professionals struggle to equip business executives with data security information.

60%+

agree that executive-level security tools can improve business executives' ability to proactively manage data risk.

Is Your Company In Peril If Critical Data Is Breached?

Where Does Accountability For Data Security Rest?

Forrester's research has shown that business decision makers are very concerned about information security and privacy risk. This is their greatest concern overall relative to other risks in their purview, including political, strategic, and financial.[1] Given how accountability for data breaches is spread, they're right to feel apprehensive. While senior-most IT leaders are the most accountable internally following a data breach, accountability shifts to (primarily) the CEO in the eyes of external stakeholders.

Delegating data security to IT teams does not absolve the responsibility business leaders have to protect data. Given recent, highly publicized executive departures across a range of industries — including media/entertainment, retail, technology, and credit risk reporting — business leaders need to acquire data security visibility and understanding like their jobs depend on it, because they do.

CEOs are most accountable following a critical data breach in the eyes of external stakeholders, such as customers, partners, shareholders, and regulators.

"Who within your organization is most likely to be held accountable internally and externally in the event of a breach or compromise to critical data and information?"

Base: 150 IT/information security and risk decision makers at organizations with 1,000 or more employees
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Agile 3 Solutions, an IBM company, November 2017

Is Your Company In Peril If Critical Data Is Breached?

With Information Assets, Opportunities And Threats Are Intertwined

With the opportunity to use data to improve business operations and customer experiences comes the threat of data compromise and loss. But before IT and business executives can take on their data security responsibilities, they must first identify their company's critical data and information — the types that are key to their success and would pose considerable risk if compromised. Good news: Respondents report that their firms are prioritizing the protection of these assets. They prioritize safeguarding corporate financial and customer data — regulated data, that in light of new regulations like GDPR, is under constant scrutiny and if compromised, would likely make headlines.

But compliance isn't enough; those in compliance may still be at risk of a breach, leaving the door open to reputational damage. And while the exposure of some information, like strategic business plans (including merger and acquisition, strategic, and long-term growth plans) and intellectual property, may not be made public, it can erode competitive differentiation and jeopardize long-term success. Nearly 20% of firms recognize this threat and are making strategic business plans and intellectual property their highest data protection priority.

"Rank the following in the order in which your organization is prioritizing its security and protection."
(Top five responses; Rank 1 represents "highest priority")

Base: 150 IT/information security and risk decision makers at organizations with 1,000 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of Agile 3 Solutions, an IBM company, November 2017

Is Your Company In Peril If Critical Data Is Breached?

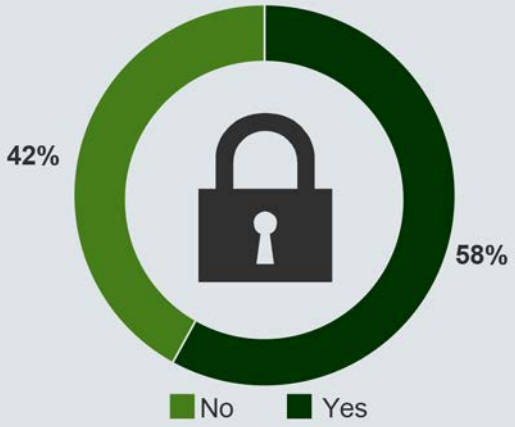
Expect Breaches To Critical Data

Despite firms' best efforts, breaches to critical data and information are common: 58% report that they've suffered from one or more breaches in the last 24 months.

- Among the 58% that have experienced a breach in the last 24 months, more (59%) report breaches in the current year than in the prior year (51%). A spike in breaches in this short period points to inadequate staff attention, procedures, and tools for a constantly evolving threat landscape.
- Among the 42% that have not experienced a breach in this period, the majority admit they're simply not aware of one. Just 36% are certain that they have not been affected. This suggests that there are breaches that may have occurred but have yet to be discovered, and that the true number of those currently affected is larger than estimated.

The median time to discover a breach is close to 100 days by some industry estimates.[2]

"Has your company experienced a breach or compromise to your company's critical data and information in the last 24 months?"



Base: 150 IT/information security and risk decision makers at organizations with 1,000 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of Agile 3 Solutions, an IBM company, November 2017

Is Your Company In Peril If Critical Data Is Breached?

A Lapse In Data Controls Is Costly

Business leaders must get in the driver's seat for incident response to contain the damage that is likely to inflict several areas of the business following a breach. The average cost per incident can exceed $3 million by some estimates, and certain costs — like brand and customer trust damage — are more difficult to quantify and take time to realize.[3] Common aftereffects respondents report include:

- **Additional security and audit requirements.** These may include the cost of repairing existing architecture, onboarding new solutions, and applying legally mandated security standards.[4]
- **High costs associated with incident response.** Affected firms should also expect costs associated with remediation and with communication to affected individuals and regulatory bodies.
- **Regulatory fines.** Regulated penalties may be significant (GDPR fines, for example, can amount to 4% of revenue or €20 million, whichever is greater). Companies must also consider the cost associated with responding to regulator-requested information.
- **Lost productivity.** Threat elimination may require downtime, and employees' attention will likely turn away from customers and growing the business to reassuring those affected and implementing new data security controls.

"Which of the following have you experienced following a breach or compromise involving critical data and information?" (Select all that apply, top responses shown)

Base: 87 IT/information security and risk decision makers at organizations with 1,000 or more employees that have experienced a breach or compromise of critical data and/or information within the past 24 months
Source: A commissioned study conducted by Forrester Consulting on behalf of Agile 3 Solutions, an IBM company, November 2017

Is Your Company In Peril If Critical Data Is Breached?

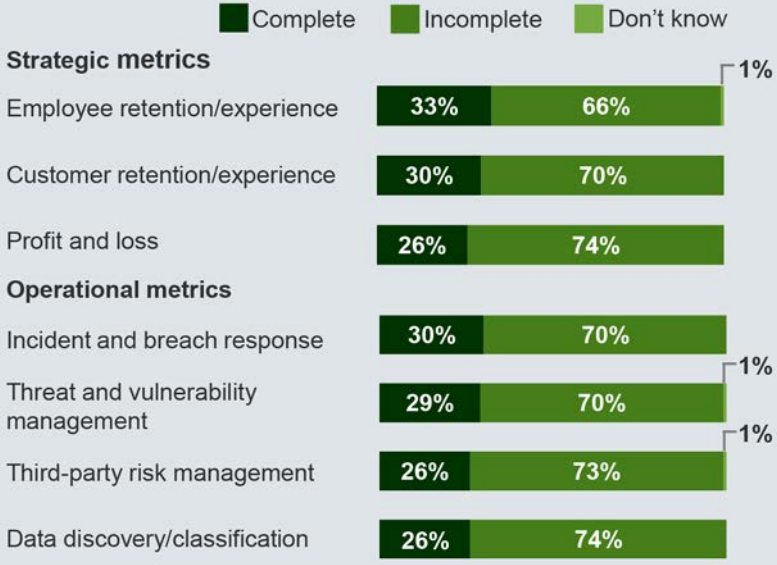
Business Leaders Need Right-Sized Data Security Visibility And Understanding

Over 70% of IT and security pros believe it's important for business executives to have visibility into a long list of data security metrics. A more effective approach is to offer a focused set of strategic and operational metrics that enable fast and effective business decisions — not tactical information best suited for front-line security staff.

- **Strategic metrics.** The highest levels of the business need profit and loss, brand, and customer loyalty impact information before, during, and after a breach. Unfortunately, two-thirds or more describe their business leaders' actual visibility into strategic metrics — employee and customer experience, profit and loss — as incomplete.
- **Operational metrics.** Operational metrics, such as incident response, threat and vulnerability management, third-party risk, and data discovery, measure how well business units interact to protect sensitive data. But just 30% or less say business leaders have complete visibility into these metrics today.

Business executives need a focused set of metrics that enable fast and effective decisions.

"What level of visibility do your non-IT executives and LOB leaders have into the following security and privacy metrics?"



Base: Varies; IT/information security and risk decision makers at organizations with 1,000 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of Agile 3 Solutions, an IBM company, November 2017

Is Your Company In Peril If Critical Data Is Breached?

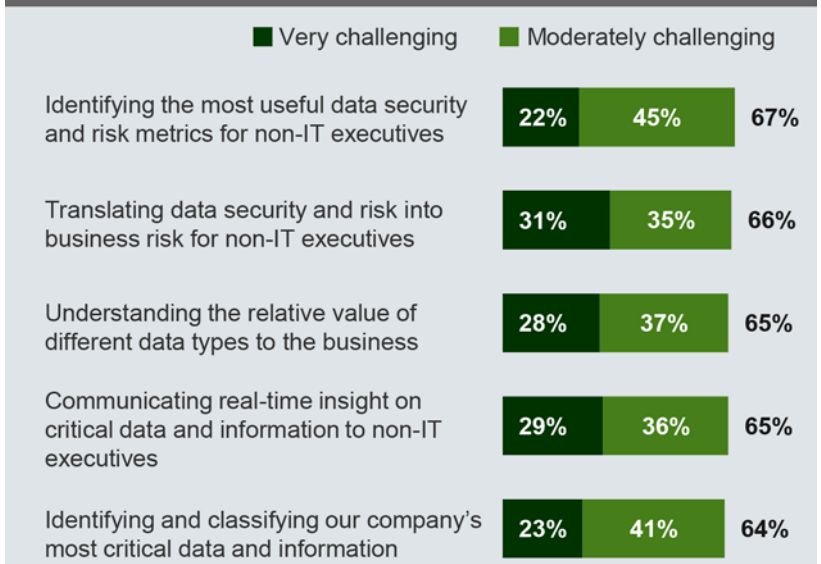
IT And Security Pros Must Become Strategic Business Partners

Business leaders need their IT and security counterparts to not only be security experts, but strategic partners. But if IT and security pros lack the right metrics, information, and approach, they will be unable to embed themselves into business conversations and positively affect data security practices.

IT and security professionals understand the importance of giving their business colleagues data security visibility that defines risk. However, roughly two-thirds encounter challenges with understanding, identifying, translating, and communicating the type of security information that business executives need. And before a successful metrics program can be developed, IT leaders need to identify and classify their firm's most critical data and information — but 64% describe this task as "very" or "moderately" challenging.

Sixty-seven percent of IT and security pros struggle to identify the most useful data security and risk metrics for non-IT executives.

"To what extent do the following present a challenge for your security and risk team(s)?" (Rate on five-point scale where 5 is "Very challenging"; top five challenges shown)



Base: 150 IT/information security and risk decision makers at organizations with 1,000 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of Agile 3 Solutions, an IBM company, November 2017

Is Your Company In Peril If Critical Data Is Breached?

The Data Protection Opportunity: Executive-Level Security Tools

Without business executive involvement, data security initiatives and budgets will suffer, leaving critical data at risk. Business leaders need visibility into where their most critical data resides, whether or not it is vulnerable, the impact it would have on the organization in the event it is compromised, and which steps to take to help prevent or mitigate an attack.

Over 60% of respondents agree that data security tools intended for a business executive-level audience would improve those leaders' ability to proactively manage data risk. In particular, respondents greatly value capabilities like a dashboard with views of business risk and affected sensitive assets, near real-time risk and exposure information, and analytics that asses risk type, among other business-friendly, highly visual, features.

Sixty-nine percent agree that a purpose-built, visual dashboard with views of business risk and affected sensitive assets can improve executives' ability to proactively manage data risk.

"To what degree would the following capabilities improve your non-IT executives' ability to proactively manage critical data risk? ("Significantly" or "Moderately" improve)

Base: 150 IT/information security and risk decision makers at organizations with 1,000 or more employees
Source: A commissioned study conducted by Forrester Consulting on behalf of Agile 3 Solutions, an IBM company, November 2017

Is Your Company In Peril If Critical Data Is Breached?

A Centralized Data Security Solution Provides Four Key Benefits

Business executives need comprehensive, continuous, and relevant data security visibility. But referencing multiple security systems and sources can be, at best, inefficient, and worst, insufficient. Granting business executives access to a centralized command center with these features in one place can lead to companywide benefits:

- A dashboard with views of business risks and affected sensitive assets.
- Near real-time risk and exposure information.
- Analytics that assess type of risk, potential impact, and affected assets.
- Security response guidance commensurate with the data's value.
- Graphic illustrations of affected information assets and business processes.
- Drill-down capabilities to uncover, analyze, and visualize data-related business risks.
- Continually updated risk registry to assess new risks and identify targeted info assets.
- Mobile capabilities with views of business risk.

"If your non-IT executives and LOB leaders had access to a centralized solution with these capabilities, which of these benefits could be realized?" (Top four shown)

Base: 150 IT/information security and risk decision makers at organizations with 1,000 or more employees
Note: Respondents were shown capabilities described in the bulleted list on this page
Source: A commissioned study conducted by Forrester Consulting on behalf of Agile 3 Solutions, an IBM company, November 2017

Is Your Company In Peril If Critical Data Is Breached?

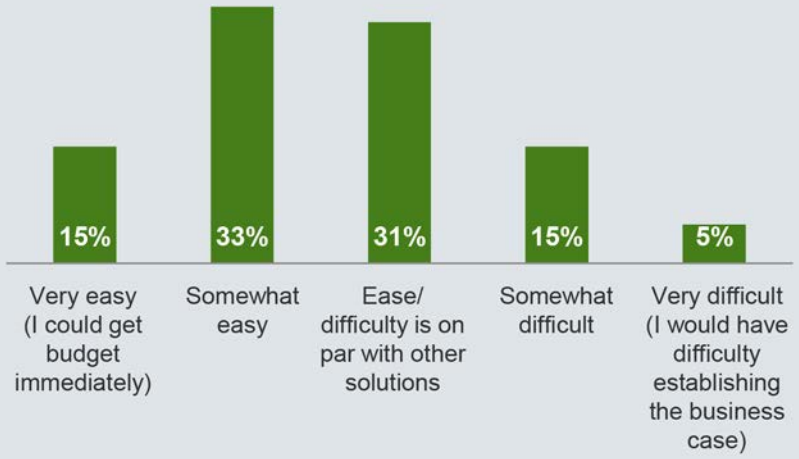
Invest in Security Controls Today To Protect Critical Data Assets

Seventy-nine percent of IT and security pros feel they can justify the business case for a centralized, business-friendly command center with these capabilities.

Investing now in data security controls that align IT, security, and the business not only help prevent costly breaches down the road, but also ensure that key stakeholders can come together today to help execute on the company's security strategy. Companies equipped with these tools will be those best positioned to protect personally identifiable data, intellectual property, and strategic plans from falling into the wrong hands.

Seventy-nine percent of IT and security pros can justify the business case for a centralized, business-friendly, data security command center.

"How easy or difficult would it be to establish the business case for a centralized solution with these capabilities?"



Base: 150 IT/information security and risk decision makers at organizations with 1,000 or more employees
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Agile 3 Solutions, an IBM company, November 2017

Conclusion

Greater cybercriminal sophistication, regulations, and customer privacy expectations are ushering in a new era of data security accountability. Now, senior business executives are primarily held accountable by external stakeholders in the event of a data compromise. It's no longer optional: Business leaders must play an active role in protecting their company's critical data assets. As recent, highly publicized breaches demonstrate, their firm's reputation and stock price, and their jobs, are at stake.

IT and security pros struggle to distinguish between tactical, operational, and strategic security priorities. However, it is imperative that they are able to communicate these very priorities to business leaders, who often lack security expertise, in a language they understand. While it may be tempting to develop a long list of metrics for everyone, for security information to be used and understood, it needs to have context for the intended audience. In the case of business executives, that means data security information linked to customers, employees, business performance, and operations delivered in a business-friendly format. Investing in tools that help bridge the communication gap can help. These solutions identify firms' most critical data and information and translate risk from a business lens. Access to these solutions can lead to faster, more effective decisions that ensure sensitive data and intellectual property continue to contribute to an organization's competitiveness and success.

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.

© 2018, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to forrester.com. [1-1444BP2]

Project Director

Sophia Christakis
Market Impact Associate Consultant

Contributing Research

Forrester's Security & Risk research group

Is Your Company In Peril If Critical Data Is Breached?

Methodology

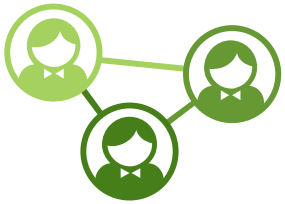
This Opportunity Snapshot was commissioned by Agile 3, an IBM company. To create this Snapshot, Forrester conducted a custom survey of 150 IT, security, and risk leaders. To qualify for the study, respondents had to be the final decision maker, part of a team making decisions, or a decision influencer for either IT/information security protection or business/IT risk management.

Respondent profile

Regions
- **33%** North America
- **33%** Europe
- **33%** Asia Pacific

Company size
- **43%** 1,000 to 4,999
- **36%** 5,000 to 19,999
- **21%** 20,000 or more

Department
- **70%** IT
- **16%** Risk management/ compliance
- **14%** Security



Job level
- **33%** C-level or vice-president
- **27%** Director
- **40%** Manager

Note: Percentages may not total 100 because of rounding.

Endnotes

[1] Source: “Security Leaders, Earn Your Seat At The Table,” Forrester Research, Inc., April 29, 2015.
[2] Source: “M-Trends 2017,” FireEye (https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html).
[3] Source: “2017 Cost of Data Breach Study: Global Analysis,” Ponemon Institute, June 2017.
[4] Source: “Calculate The Business Impact And Cost Of A Breach,” Forrester Research, Inc., August 31, 2017.