Gauge Your Data Security And Privacy Maturity

Assessment: The Data Security And Privacy Playbook

by Enza Iannopollo and Heidi Shey
October 5, 2018

Why Read This Report

To transition from an organization that treats privacy and data security as compliance requirements to achieve the lowest possible cost, to one that champions privacy and uses its technology prowess to differentiate the brand, you need to know where to start. This report guides security, privacy, and other risk pros through Forrester's Data Security And Privacy Maturity Assessment so you can gauge where your firm is on its journey and discover which core competencies you need to strengthen or develop.

Key Takeaways

Master Four Competencies To Lead In Data Security And Privacy

Forrester has identified four competencies that every security, privacy, or other risk pro must tackle: oversight, technology, process, and people.

Key Activities Underpin Each Of The Four Competencies

To assess the maturity of each activity — and therefore the overall competency — you must assess each statement using a Likert Scale to determine if you agree or disagree.

Take The Self-Assessment To Determine Your Current Maturity

Completing our 15-minute questionnaire tells you how close you are to Forrester's vision of using data security and privacy as a competitive differentiator — if you're in the beginner, intermediate, or advanced stage — in each of the four competencies. Use research specific to your needs to plan your road map.

Gauge Your Data Security And Privacy Maturity

Assessment: The Data Security And Privacy Playbook

by Enza Iannopollo and Heidi Shey
with Stephanie Balaouras, Elsa Pikulik, and Peggy Dostie

October 5, 2018

Table Of Contents

Related Research Documents

Build Your Privacy Organization For Customer Data Management

Calculate The Business Impact And Cost Of A Breach

The Future Of Data Security And Privacy: Growth And Competitive Differentiation

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Data Security And Privacy Require Mastery Of Four Competencies

Hacked customer data can erase millions in profits; stolen IP can destroy competitive advantage; and unnecessary privacy abuses can bring unwanted scrutiny, regulatory fines, and tons of customer complaints.[1] Too many organizations fail to make customer trust a focal point of their data security and privacy strategy — a necessity in today's data economy where savvy customers are increasingly concerned about their privacy and a business' ability to protect them from cybercriminals, fraudsters, dubious third parties (e.g., Cambridge Analytica), and even unwarranted government surveillance. And too many organizations treat all their data the same, unable to identify the IP that underpins the company's differentiation and long-term financial viability.

Security and privacy leaders must help their organizations transcend basic compliance and fiduciary responsibilities to proactively protect customers, employees, and the firm's IP from complex privacy abuses and more-sophisticated cyberattacks. Mature organizations see themselves as privacy champions and recognize that data security and privacy does much more than reduce costs: It drives revenue and growth.[2] Mature organizations formalize privacy programs that bring together cross-functional teams and IT to establish privacy objectives and operationalize key workflows. They prioritize investments in capabilities that automate privacy workflows and allow them to detect, remediate, and respond to more-sophisticated attacks from both organized cybercriminals and fraudsters.[3] This assessment will uncover how mature you are against four key competencies of The Forrester Data Security And Privacy Maturity Assessment (see Figure 1):

- **Oversight.** Oversight consists of four main areas or activities: strategy, alignment, performance management, and program. These areas are critical to help security and privacy leaders define and deliver on privacy objectives according to available resources and business needs. It also helps organizations develop ways to evaluate their performance levels and verify that goals are met.
- **Technology.** Data security and privacy technologies encompass solutions and capabilities that enable organizations to: 1) discover, classify, and map sensitive data throughout the enterprise; 2) detect and block exfiltration and accidental loss of sensitive data; 3) obfuscate sensitive data; 4) restrict access to sensitive data; 5) achieve, demonstrate, and maintain compliance; and 6) empower customers to exercise their privacy rights.
- **Process.** Process describes the core workflows needed to manage privacy compliance and protect data with strong security controls. It includes critical processes such as establishing privacy by design across the enterprise and also includes legal and process controls that help address privacy requirements when working with partners, law enforcement, and entities overseas.
- **People.** This competency focuses on the human factors impacting privacy practices. It includes mechanisms to set expectations for behavior internally to meet privacy demands, recruiting and retaining a diverse staff of highly qualified individuals, and establishing a culture where executives across the organization act as privacy champions and foster cross-functional cooperation.

FIGURE 1 The 20 Activities That Gauge Your Data Security And Privacy Maturity

Oversight
1) The organization's privacy strategy contains clear privacy objectives based on current conditions, available resources, the needs of the business, and customer expectations.
2) The privacy strategy is directly linked to business strategy, and privacy is seen as a key element of business success.
3) Privacy efforts are continuously measured and adjusted for business performance, customer sentiment, risk profile, and regulatory standing.
4) There are governance structures in place to understand privacy expectations and requirements, define roles and responsibilities, forecast budgetary needs, and allocate resources.
Technology
5) The organization can retain control of and secure data across locations, hosting models, and user populations via technology such as encryption and other obfuscation techniques, key management, rights management, secure file sharing tools, cloud security gateways, etc.
6) The organization can inspect data at rest, in use, and in motion to detect and respond to deviations from information handling policy (e.g., accidental data loss or data exfiltration), monitor user interaction with data, and address insider threats.
7) The organization can strictly control how employees, contractors, and other parties can access private data based on business need and risk management objectives.
8) The organization can determine when it's necessary to conduct a privacy impact assessment and use technology and appropriate frameworks to perform and document the assessment.
9) The organization can identify where it stores or processes sensitive data and label it according to attributes that dictate the level and type of privacy controls that should be applied.
10) The organization can identify data and deploy controls to address customer requests for personal data deletion (e.g., the right to be forgotten), data access, data portability, and other similar requests as mandated by regulatory requirements (GDPR and CCPA) and customers' expectations.
11) The organization has continuous visibility into data flows, including collection and origin, processing (technology used to perform actions, hosting, access), storage, and third-party sharing.
12) The organization can archive and electronically delete data according to retention policies and respond to discovery requests triggered by events such as litigation, internal investigations and audits, freedom of information requests, and regulatory action.

FIGURE 1 The 20 Activities That Gauge Your Data Security And Privacy Maturity (Cont.)

Process
13) The organization can continuously execute a cross-functional process to assess data privacy risks as they emerge from data processing activities across business units and apply policies to reduce exposure of personal data.
14) The organization can routinely execute a process to gather visibility on third parties' cybersecurity and privacy practices, including compliance with relevant regulations, and assess and remediate third- party risk with an approach that involves technical, legal, contractual, and other remedies as necessary.
15) The organization can continuously execute a process to monitor data flows that involve transfer of data from one jurisdiction to another and accurately flag and remediate situations of high security, privacy, or regulatory risk in a way that employs technical, legal, regulatory, and other remedies as appropriate.
16) The organization has implemented and communicated processes that enable customers to conveniently exercise their privacy rights, including data subject rights, consent collection and consent withdrawal, object to processing, consent to third-party data sharing, etc.
People
17) The organization can instill an appreciation of privacy among its employees and enforce accountability for helping to protect customer data.
18) The organization has sufficient staff resources and expertise to support data security and privacy objectives.
19) The organization can recruit security and privacy talent from diverse backgrounds and retain talented staff by promoting inclusion, providing challenging work and opportunities for personal and career development, and offering competitive salaries and benefits.
20) Executive leaders champion data security and privacy and are accountable for its success in their groups/teams. Their efforts bolster culture and facilitate effective cross-functional collaboration across the organization.

Recommendations

Plot Your Data Security And Privacy Maturity

Use our assessment to gauge your maturity against the four competencies we've identified. By understanding where you stand today you will know if you need to:

- **Improve foundational processes and deploy essential security controls.** If you're a beginner, you're busy building the groundwork that will enable your security and privacy posture to mature in the future. Focus on building a solid foundation. First, formalize processes and procedures in simple policies that you can expand and measure in the future. Second, adopt security controls that protect the organization from the most likely attacks, abuses, and employees' mistakes.
- **Prioritize investments in automation and manage risks more efficiently.** If you're at the intermediate level, your focus is on becoming more sophisticated. You must: 1) carefully select and gradually introduce automated solutions to manage privacy and respond to security threats and attacks; 2) put metrics in place to measure the effectiveness of your actions, and align your security and privacy programs to business goals and direction; and 3) treat third-party risk management as a core element of program.
- **Grow corporate security and privacy culture to drive competitive differentiation.** If you're an advanced organization, you're not a "follower" anymore. You're a leader. Dedicate your efforts to: 1) nurture your corporate culture for privacy and security — proactively involve each employee with a continuous and constructive campaign; 2) engage with other business leaders to craft a strategy for creating awareness in the marketplace about your security and privacy maturity; and 3) share and promote best practices with your third parties and require that they improve their own security and privacy posture as a condition of doing business with you. Take the assessment for more insights into your maturity level and read the advanced level report to learn what's next on the way to excellence.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iOS and Android.
Stay ahead of your competition no matter where you are.

Supplemental Material

Online Resource

The online version of this report includes a maturity assessment. Click the link at the beginning of this report on Forrester.com to access the assessment.

Endnotes

[1] Source: Alex Hern, "European regulators report sharp rise in complaints after GDPR," The Guardian, June 26, 2018 (https://www.theguardian.com/technology/2018/jun/26/european-regulators-report-sharp-rise-in-complaints-after-gdpr).

[2] Data is the lifeblood of digital businesses; protecting it from theft, misuse, and abuse is the top responsibility of every security and privacy leader. Hacked customer data can erase millions in profits, stolen IP can destroy competitive advantage, and privacy abuses can bring unwanted scrutiny, regulatory fines, and damaged reputations. Security and privacy pros must ensure that security travels with the data across the business ecosystem, position data security and privacy as competitive differentiators, and build a new kind of customer relationship. See the Forrester report "The Future Of Data Security And Privacy: Growth And Competitive Differentiation."

[3] How companies handle and protect consumer data privacy is much more than a compliance issue. Privacy is a competitive differentiator. This requires oversight and clear lines of privacy responsibility and accountability. S&R pros can't tackle this alone and must partner with their business peers. This report outlines the key capabilities necessary to build a privacy program that effectively manages customer data privacy. See the Forrester report "Build Your Privacy Organization For Customer Data Management."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.