

Secure Customers And Protect Your Brand

Executive Overview: The Cybersecurity And Privacy Playbook

by Laura Koetzle

September 25, 2018

Why Read This Report

Today, CIOs and CTOs are transforming the foundations of their business with technology; for that transformation to succeed, you must transform your cybersecurity and privacy practices simultaneously. This report provides an overview of Forrester's framework for securing your customers, protecting your brand, and driving differentiation: the cybersecurity and privacy playbook.

Key Takeaways

Cybersecurity And Privacy Drive Business Growth

Risk-aligned, business-enabling, and forward-thinking security and privacy practices can help you win, serve, and retain customers.

Excel At Four Competencies To Secure Customers And Protect The Brand

Forrester's four tried-and-true competencies — people, process, technology, and oversight — remain the best way to attack the problem.

Secure Customers And Protect Your Brand

Executive Overview: The Cybersecurity And Privacy Playbook



by [Laura Koetzle](#)

with [Stephanie Balaouras](#), [Jinan Budge](#), and [Elsa Pikulik](#)

September 25, 2018

Cybersecurity And Privacy *Do* Drive Business Growth

Admit it: A few years ago, you were one of the CIOs who could barely stop themselves from rolling their eyes when your chief information security officer (CISO) or head of privacy mentioned for the umpteenth time that cybersecurity and privacy were business-critical. No longer: Now, you're likely spending more than 10% of your technology budget on cybersecurity and privacy for related staff, services, and technology, and you'll need to invest more as your IT transformation progresses.¹ That's the right thing to do, because strong cybersecurity and privacy practices not only insulate your firm from harm, they also help differentiate your brand and help your firm safely serve markets that competitors can't. This is because:

- › **Consumers worldwide care how you use their data, and they vote with their wallets.** More than 60% of online adults in France, Germany, Italy, Spain, and the UK say that they're likely to ask companies to delete information about them.² But it isn't just Europeans who care about privacy; few online adults in Canada, Japan, or Australia are comfortable with companies sharing or selling information about them.³ One in ten US online adults report abandoning an online purchase because the site asked for too much personal information.⁴
- › **Suppliers and B2B customers won't let your poor security become their problem.** According to our survey of network security decision makers, third-party incidents caused 17% of confirmed breaches in 2017.⁵ This is why 65% of security decision makers rated ensuring that business partners and third parties comply with their internal security requirements as a high or critical priority, and it's why your CISO is investing in third-party risk management.⁶ This also means that the CISOs at your suppliers and customers are putting *your* firm under a microscope. If your cybersecurity and privacy efforts don't meet their standards — as when Equifax's poor patch management imperiled everyone's identity verification processes — your firm might find itself out in the cold.⁷
- › **Regulators will penalize you if you don't protect your customers properly.** Look no further than the much-cited EU GDPR maximum fines of 4% of global revenue or €20 million, whichever is higher.⁸ EU data protection authorities have beefed up to enforce the new rules; for example,

FORRESTER

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

© 2018 Forrester Research, Inc. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Unauthorized copying or distributing is a violation of copyright law. Citations@forrester.com or +1 866-367-7378

Secure Customers And Protect Your Brand

Executive Overview: The Cybersecurity And Privacy Playbook

the Irish data protection commissioner received 55% more funding in 2018 than in 2017.⁹ And jurisdictions around the world (Brazil and California being but two of the most recent) are passing their own GDPR-like data protection laws.¹⁰

Master Four Battle-Tested Cybersecurity And Privacy Competencies

It's easy to get distracted by the constant upheaval of new and frightening cybersecurity and privacy threats. But CIOs, CISOs, and heads of privacy should stick to the four fundamental competencies Forrester has used since 2007:

- › **People: Use cultural efforts to foster an educated, engaged workforce.** Hire people with sound ethical instincts and reward them for finding, communicating, and fixing problems. They'll treat cybersecurity and privacy as core values.
- › **Process: Pursue security and privacy by design.** "Built-in, not bolt-on" has rightly been a rallying cry for CISOs and privacy leaders for years. Technology leaders should seize the opportunity to build cybersecurity and privacy into their firm's products and services as they develop them.¹¹
- › **Technology: Avoid expense-in-depth by focusing on the four things that matter.** The cybersecurity industrial complex loves to scare leaders into buying (inevitably disappointing) silver bullets. Ignore all fearmongering. As a CIO, the four critical privacy and security technology areas for your technology transformation strategy are data governance, data security, cloud governance, and technology innovation.¹²
- › **Oversight: Embed cybersecurity and privacy specifics into strategy and governance.** Technical controls are useful and necessary, but it's critical to define, articulate, measure, and address cybersecurity and privacy risks across your business and your ecosystem of partners and suppliers.¹³ Without oversight, you cannot understand your current maturity and performance, identify gaps, or create a detailed road map for continuous improvement.

Secure Customers And Protect The Brand With This Playbook

Forrester's cybersecurity and privacy playbook is a tightly integrated set of reports that helps technology leaders secure customers, protect the brand, and drive business growth. The playbook accompanies CIOs throughout the process, from building an initial shared vision to executing it and advancing to the next level of maturity. It does this by means of:

- › **Six foundational reports.** These reports give you all the insights you need to integrate cybersecurity and privacy into the broader technology transformation you're leading. This executive overview explains how to use the playbook. The [vision report](#) makes the case that the intersection of the data economy, artificial intelligence, and automation will require you to prioritize data integrity and ethical decision making. The [assessment](#) shows you how to gauge your maturity in each of the four competencies so you know what to do next. The [strategy report](#) provides CIO-level tools

Secure Customers And Protect Your Brand

Executive Overview: The Cybersecurity And Privacy Playbook

to drive cybersecurity and privacy improvement. The business case report offers a template for pitching cybersecurity and privacy investments to your stakeholders. Finally, the benchmarks report presents the assessment results of your peers so you can see where you fall on the continuum.

- › **A series of three reports for each of the four competencies.** Once you've assessed your organization's maturity, these reports will guide you through the three stages of maturity — beginner, intermediate, and advanced — for each of the four competencies.

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.

Endnotes

¹ Data breaches, stiff competition for talent, and decentralized tech spending are still major challenges for security leaders' budgets. Forrester compares the budgets of security decision makers at firms spending up to 10%, 11% to 20%, and 21% to 30% of their overall tech budget on information security technologies. Security leaders can use these budget ranges as a starting point and compare their product, service, staffing, and other allocations with those of similar firms. See the Forrester report "[Security Budgets 2018: Uncertainty Trumps Normalcy.](#)"

Secure Customers And Protect Your Brand

Executive Overview: The Cybersecurity And Privacy Playbook

- ² When we asked online adults how likely it was that they would ask companies to delete information about them, the percentages of respondents selecting “agree” or “strongly agree” were 61% in France, 65% in Germany, 68% in Italy, 69% in Spain, and 62% in the UK. Source: Forrester Analytics Consumer Technographics® Global Online Benchmark Survey (Part 2), 2018.
- ³ When we asked online adults if they were comfortable with companies sharing and selling their data and information about their online activities, the percentages of respondents selecting “agree” or “strongly agree” were just 21% in Australia, 12% in Japan, and 11% in Canada. Source: Forrester Analytics Consumer Technographics Asia Pacific Survey (Technology, Media, And Telecom; Financial Services), Q3 2018 and Forrester Analytics Consumer Technographics Global Online Benchmark Survey (Part 2), 2018.
- ⁴ Source: Forrester Analytics Consumer Technographics North American Retail And Travel Benchmark Recontact Survey 1, Q3 2017 (US).
- ⁵ Base: 1,364 breaches confirmed by 330 North American and European network security decision makers whose firms have had a security breach in the past 12 months. Source: Forrester Analytics Global Business Technographics Security Survey, 2017.

Managing the cybersecurity postures of your third parties is a crucial aspect of risk management. Third-party cyber-risk-scoring solutions are helping S&R pros identify, measure, and mitigate the cyber risks across their third-party ecosystem. Forrester reviews the three types of solutions and how they can help prevent your organization from becoming the next publicized third-party breach. See the Forrester report [“Protect Your Extended Ecosystem With Third-Party Cyber-Risk Scoring.”](#)

- ⁶ Source: Forrester Analytics Global Business Technographics Security Survey, 2017.

Managing the cybersecurity postures of your third parties is a crucial aspect of risk management. Third-party cyber-risk-scoring solutions are helping S&R pros identify, measure, and mitigate the cyber risks across their third-party ecosystem. Forrester reviews the three types of solutions and how they can help prevent your organization from becoming the next publicized third-party breach. See the Forrester report [“Protect Your Extended Ecosystem With Third-Party Cyber-Risk Scoring.”](#)

- ⁷ It doesn't matter if third parties supply you with data, technology, or services: If they touch your customers' or employees' personal data, their security and privacy postures directly affect your business, security, and ability to comply with regulations and customer expectations. This report explains how GDPR affects traditional third-party risk management and how you need to adapt. See the Forrester report [“Manage Third-Party Risk To Achieve And Maintain GDPR Compliance.”](#)

Source: Enza Iannopollo, “Regulators Will Fine Facebook Only A Small Amount, But The Size Matters Less Than You Think . . . At Least This Time,” Forrester Blogs, July 11, 2018 (<https://go.forrester.com/blogs/regulators-will-fine-facebook-only-a-small-amount-but-the-size-matters-less-than-you-think-at-least-this-time/>).

- ⁸ EU GDPR = the European Union's General Data Protection Regulation.
- ⁹ Source: Charlie Taylor, “Data commissioner welcomes ‘critical’ €4m budget rise,” The Irish Times, October 12, 2017 (<https://www.irishtimes.com/business/technology/data-commissioner-welcomes-critical-4m-budget-rise-1.3252310>).
- ¹⁰ Source: Katherine E. Armstrong, “Brazil Adopts New Privacy Law Similar to GDPR,” DBR on Data blog, August 28, 2018 (<https://www.lexology.com/library/detail.aspx?g=2b0a61cb-d3ed-4027-a00a-b697eb2df062>).

Source: Daisuke Wakabayashi, “California Passes Sweeping Law to Protect Online Privacy,” The New York Times, June 28, 2018 (<https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html/>).

- ¹¹ Privacy is not only possible but essential for building trust. Context is key — businesses crave insight into the context in which consumers are using their products, and consumers want businesses to deliver contextually relevant services. Contextual privacy enables companies to negotiate the collection and use of personal data to ensure a fair value exchange for both parties. This report explains contextual privacy, why B2C marketing pros must adopt it, and how to implement best practices. See the Forrester report [“The New Privacy: It's All About Context.”](#)

Secure Customers And Protect Your Brand

Executive Overview: The Cybersecurity And Privacy Playbook

¹² 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.](#)”

¹³ In reaction to sweeping regulations and massive corporate failures, governance, risk management, and compliance (GRC) efforts have evolved slowly over the past 15 years. However, in the next five years, unprecedented changes in business and technology will demand much more sophisticated, strategic, and proactive GRC capabilities. This report dissects the risk and compliance implications of today’s and tomorrow’s biggest trends, with practical advice to help risk management pros build a program to usher their firms more safely to success. See the Forrester report “[GRC Vision 2017-2022: Customer Demands Escalate As Regulators Falter.](#)”

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.