The State Of Data Security And Privacy, 2020

Benchmarks: The Data Security And Privacy Playbook

by Heidi Shey

February 27, 2020

Why Read This Report

This data-driven report outlines breach trends, data security and privacy technology adoption trends, and related trends in global firms for 2019 through 2020. Understanding these trends and their implications will help security and risk (S&R) executives examine, and adjust as necessary, their own plans for data security and privacy.

Key Takeaways

Insider Threats And Lost/Stolen Assets Caused Their Fair Share Of Breaches In 2019
Internal incidents are still more likely to be caused by malicious intent, while the percentage of breaches caused by lost or stolen assets like laptops and smartphones increased.

Authentication Credentials Became An Increasingly Attractive Target For Attackers
Personally identifiable information (PII) remains a popular target of compromise. However, in 2019, we saw authentication credentials take the No. 2 spot, followed closely by intellectual property (IP).

Compliance Remains A Primary Driver For Technology Investment
Current technology adoption and planned adoption today focuses on various types of encryption technologies as well as privacy management tools. Best-of-breed versus a platform/portfolio approach is an ongoing consideration.

FOR SECURITY & RISK PROFESSIONALS

The State Of Data Security And Privacy, 2020

Benchmarks: The Data Security And Privacy Playbook

by Heidi Shey
with Amy DeMartine, Enza Iannopollo, Kate Pesa, and Peggy Dostie
February 27, 2020

Table Of Contents

Related Research Documents

The Forrester Tech Tide™: Data Security And Privacy, Q3 2019

Gauge Your Data Security And Privacy Maturity

The State Of Data Security And Privacy: 2018 To 2019

FORRESTER®

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

Insiders And Lost Devices Are Still Catching Firms By Surprise

In addition to conducting a maturity assessment to gauge where your capabilities and practices for data security and privacy are today and where to focus your priorities for increasing maturity, organizations can learn from the patterns seen behind data breaches, data exposure, and data misuse to evaluate their current practices and controls for data protection. Among breaches in the past 12 months, 46% involved insiders like employees and third-party partners (see Figure 1). This is consistent with what we saw in 2018. News headlines of insiders stealing trade secrets from companies like Hershey, Philips, and Tesla prime us to assume that insider threats are threats of malicious intent, but the reality is that inadvertent misuse of data and lost devices cause a fair share of incidents and breaches.[1] In 2019, our data showed that:

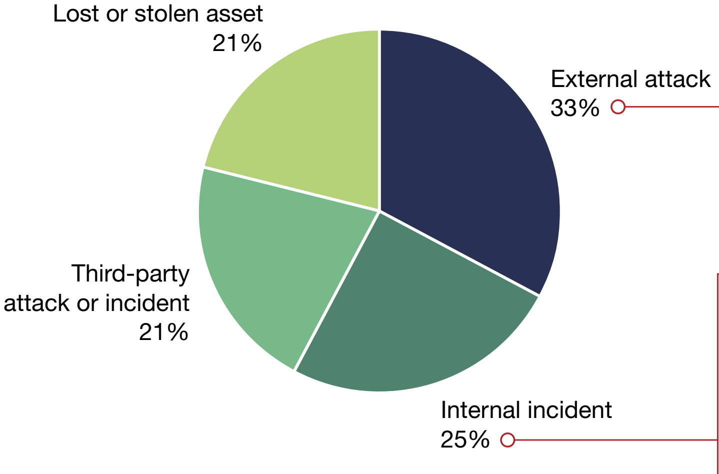
› **Internal incidents are due to inadvertent misuse almost as much as malicious intent.** According to global security decision makers, nearly half of the breaches caused by internal incidents were the result of abuse or malicious intent.[2] The decrease in malicious intent from 57% in 2018 to 48% in 2019 means that inadvertent misuse is on the rise, from 35% in 2018 to 43% in 2019.[3] As we focus on how to detect and respond to insider threats, we must not lose sight of how we approach our human firewall with building a strong security culture.[4]

› **Lost or stolen assets have jumped as a cause of breaches.** Whether the devices are corporate-issued or bring-your-own, the loss or theft of assets like smartphones and laptops were involved in 21% of the breaches reported by global security decision makers in 2019, compared with 15% in 2018.[5] Devices are an employee's window for accessing data. It's critical to have processes and capabilities to manage these endpoints, supporting your data security efforts with capabilities like setting baseline security policies (e.g., requiring device passcode, OS updates), enabling risk-based conditional access, and encryption.[6]

› **The top three data types compromised reflect their value.** PII remains the type of data that global security decision makers most often say has been compromised or breached; IP is also high on the list, coming second in 2018 and third in 2019 (see Figure 2).[7] While PII and IP have been mainstays at the top of the list for a while, authentication credentials took second place in 2019, mentioned by 35% of decision makers, up from 27% (and fourth place) in 2018. Why bother breaking in when you can log in?

FIGURE 1 Breakdown Of Confirmed Breaches In 2019

Causes of confirmed breaches in the past 12 months



The most common external attacks focused on software vulnerabilities (42%), web applications (35%), and use of stolen credentials (27%).*

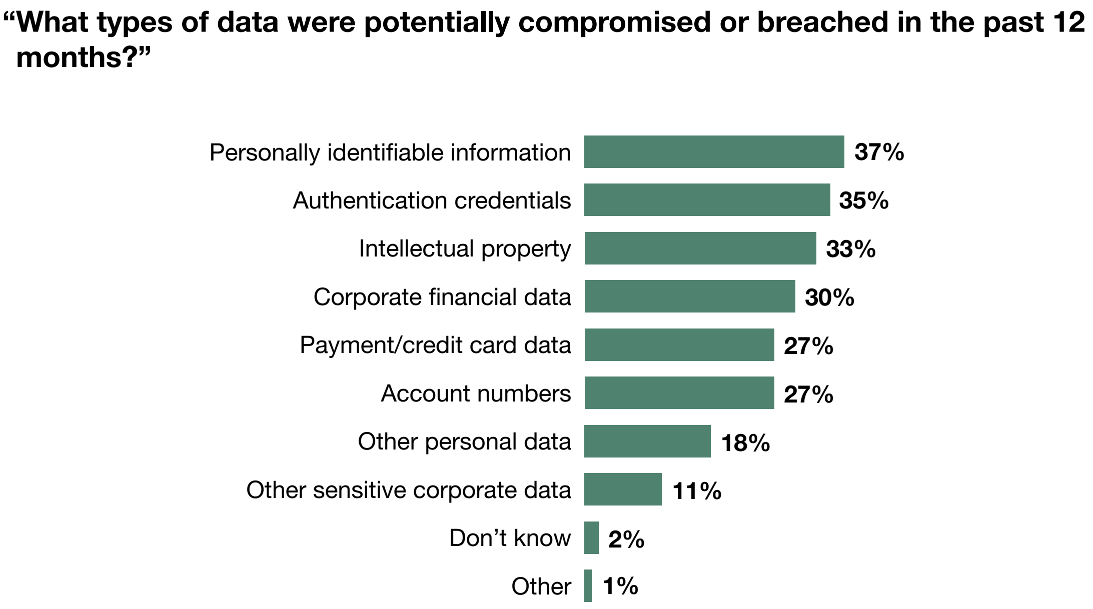
In these cases, 48% were attributed to malicious intent, 43% to inadvertent misuse or accident, and 9% to a combination of both.

Base: 3,594 breaches confirmed by 629 security decision makers with network, data center, app security, or security ops responsibilities whose firms experienced a breach in the past 12 months

Source: Forrester Analytics Global Business Technographics® Security Survey, 2019

*Respondents could choose more than one category; these are the top three response categories.

FIGURE 2 Top Data Types Compromised In The Past 12 Months



Base: 763 global security decision makers whose organization has experienced a breach in the past 12 months

Source: Forrester Analytics Global Business Technographics® Security Survey, 2019

Data Security And Privacy Tech Adoption Leans On Compliance

Every investment you make for cybersecurity and privacy is to protect data. Forrester defines data security and privacy technology as technologies that directly touch the data itself and that help organizations: 1) understand where their data is located and identify what data is sensitive; 2) control data movement as well as introduce data-centric controls that protect the data no matter where it is; and 3) enable least privilege access and use. This still encompasses a wide range of technologies.[8]

To address concerns from data breaches involving authentication credentials, you can enable multifactor authentication to mitigate risks of credential stuffing and explore passwordless authentication methods such as biometrics, tokens, keys, or Auth0-related solutions for employees.[9] To protect your PII and IP, the appropriate choice or combination of choices of specific data security technologies will depend on whether this data is in an unstructured or structured format. Common controls include encryption and data loss prevention. When we take a deeper dive into core technology adoption trends, we see that:

- **Encryption adoption holds steady as a cornerstone for data protection.** When asked what encryption technologies their firm has adopted, global security decision makers most often cited email (63%), database (60%), and cloud encryption (61%) (see Figure 3). Around one in five decision makers say that their firm plans to implement a number of types of encryption, including email, database, cloud, media, full-disk, and file-level encryption.[10] This is no surprise, as some regulations — like HIPAA, GLBA, and CCPA — have specific encryption requirements. For regulations that do not specifically mention encryption, like GDPR, many organizations still look to encryption as a key control and safeguard for data.

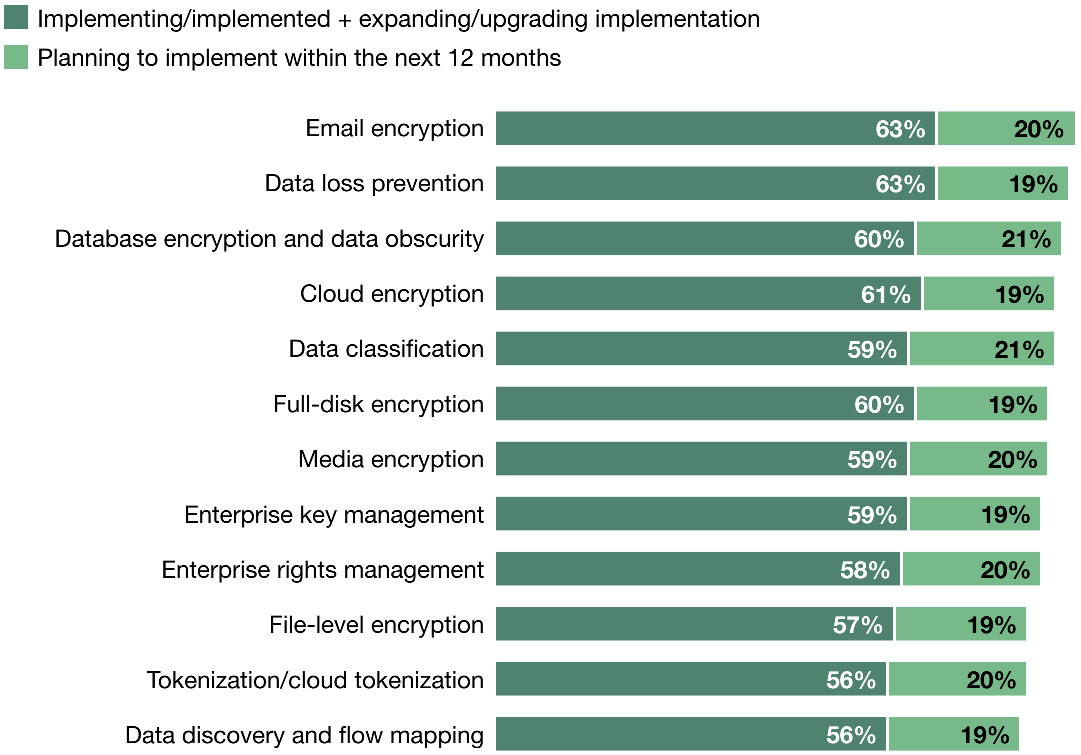
- **Data loss prevention (DLP) is not dead.** DLP as a technology capability persists because it is still a means to help enforce policies for data movement, report violations, and inform users of what is appropriate policy if they inadvertently violate it. While prior deployments primarily focused on preventing accidental data loss, added functionality today can also support insider threat use cases. The question is how we define DLP as it evolves; it's a feature, a product, a service, and it's also an approach supported by other (non-DLP) capabilities like access control or de-identification. Forrester client questions about DLP and DLP alternatives comprise a large number of data security related inquiries today.

- **Protecting data in the cloud starts before data moves to the cloud.** Private cloud, infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) all require data protection. As companies move critical data from on-premises to cloud, security considerations include securing access to the console, configuration of the cloud, connectivity/networking, encrypting cloud data, and container security.[11] Today, 28% of global security decision makers say that one of their primary methods of protecting these environments is to encrypt data before moving it to the cloud (see Figure 4).

- **Privacy regulations drive new categories of tech purchasing.** GDPR and CCPA have been a catalyst for technology investments as firms prepare to comply with regulatory requirements and develop their programs for sustained compliance.[12] Among global security decision makers, 49% indicated that they have invested in privacy management software to comply with data protection regulations (see Figure 5). They also often report investing in data discovery and classification (45%) and other data security controls (44%) to help fulfill their compliance obligations. While these can help to support your program, technology alone is not the solution. Solid processes and policies are required to deliver meaningful compliance.[13]

FIGURE 3 Core Data Security Technologies See Similar Levels Of Interest For Plans To Adopt

"What are your firm's plans to adopt the following data security and information risk management technologies?"



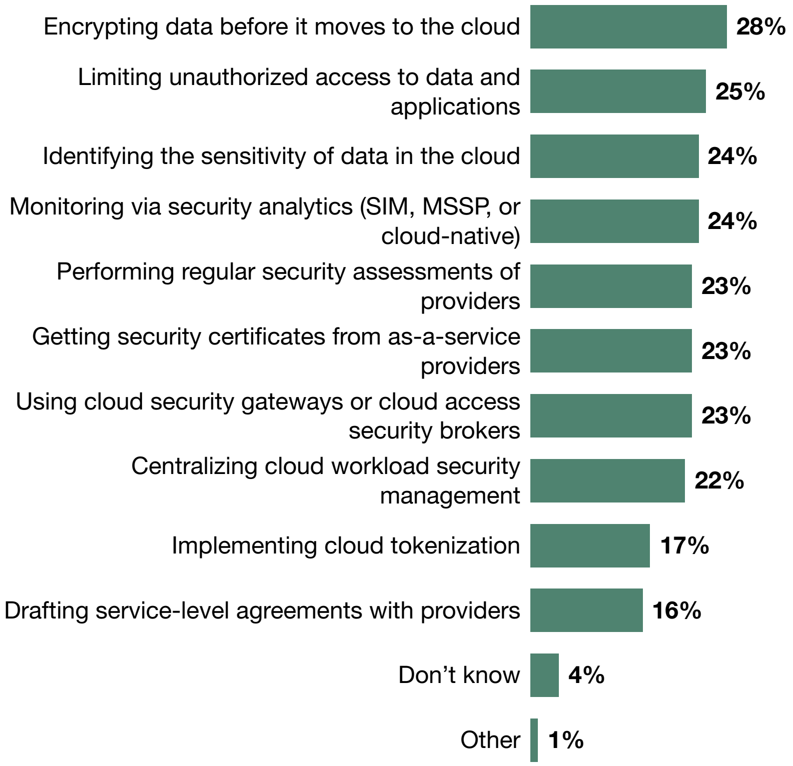
Base: 1,003 global security decision makers with client, endpoint, data, or mobile security responsibilities

Note: Not all response categories are shown.

Source: Forrester Analytics Global Business Technographics® Security Survey, 2019

FIGURE 4 Firms Rely On A Variety Of Controls And Approaches To Protect Data In The Cloud

"How does your firm primarily protect as-a-service environments offered via cloud deployment?"

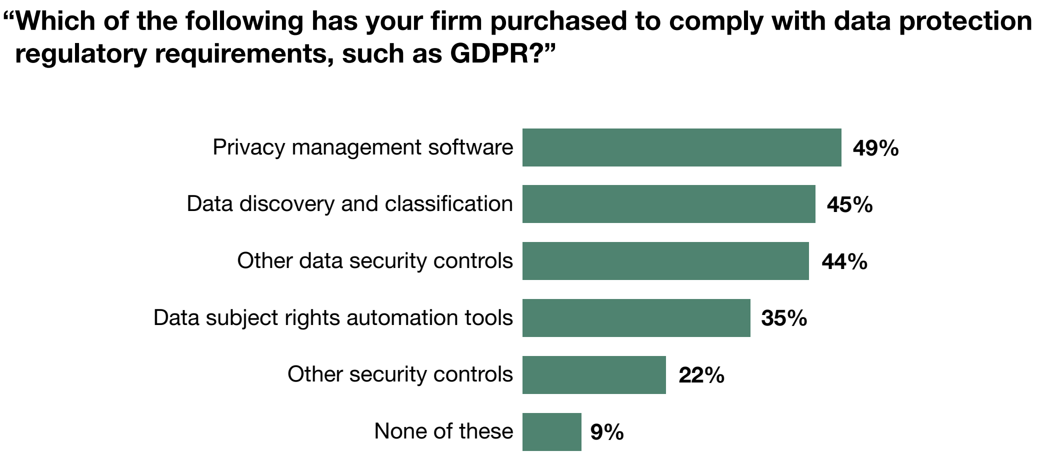


Base: 3,438 global security decision makers

Note: Not all response categories are shown.

Source: Forrester Analytics Global Business Technographics® Security Survey, 2019

FIGURE 5 Privacy Drives Tech Investment For Program Management, Defining Data, And Data Security



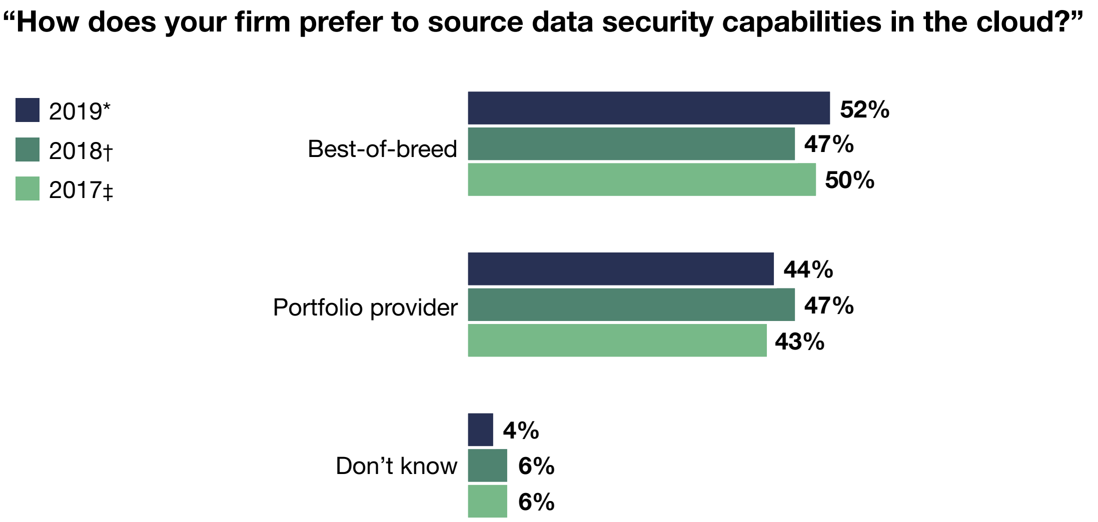
Base: 3,890 global security decision makers
Source: Forrester Analytics Global Business Technographics® Security Survey, 2019

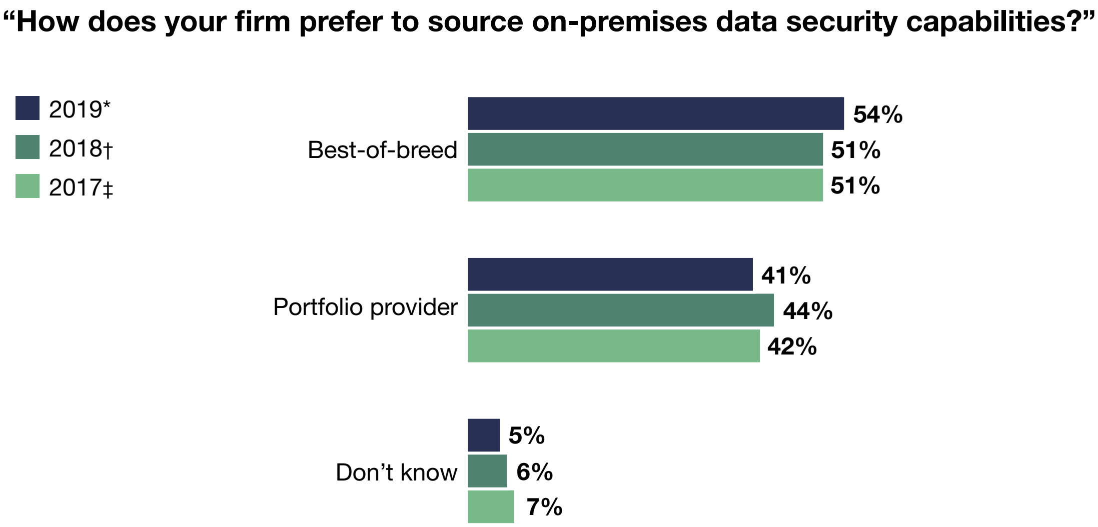
Preference For Best-Of-Breed Versus Portfolio/Platform Is An Ongoing Consideration

Amazon, Google, Microsoft have disrupted the security market landscape, emerging as new giants.[14] A few years ago, no one would have pointed to any of these tech titans as security vendors. Today, they increasingly compete with best-of-breed security technology vendors and offerings. For data security, Microsoft in particular stands out, based on Forrester client inquiries. Other major vendors like Google, IBM, and Symantec have also built a portfolio of offerings for data security.[15]

In terms of sourcing security technologies and capabilities, global security decision makers say their firms have a slight preference for best-of-breed providers regardless of whether the context is in the cloud or on-premises (see Figure 6). In 2019, slightly more than half of security decision makers indicated that they prefer best-of-breed providers in the cloud (52%) and on-premises (54%). Dedicated data security technologies continue to hold their appeal to meet specific needs. A portfolio/platform approach has its benefits and appeal, providing native capabilities in a platform or a portfolio of integrated capabilities, that can also be more cost effective and/or easier to manage.

FIGURE 6 In The Cloud And On-Premises, Many Firms Prefer Best-Of-Breed Options For Data Security





*Base: 2,260 to 2,322 global security technology decision makers
†Base: 1,600 to 1,643 global security technology decision makers
‡Base: 2,044 to 2,089 global security technology decision makers
Note: Percentages may not total 100 due to rounding.
Source: Forrester Analytics Global Business Technographics® Security Surveys, 2017 to 2019

Recommendations

Use Benchmarks As A Starting Point, Not An End Goal, **For Analysis**

The data in this report provides a view of what enterprises are spending and doing today for data security. However, each organization is unique due to its size, industry, long-term business objectives, and tolerance for risk. While it's helpful to see what other firms may be spending and doing, it's critical that S&R pros don't become prisoners of the data. Consider the benchmarks in this report as a guide, where the key trends and takeaways serve as a starting point for analyzing your own budget and technology adoption plans for data security and privacy. Based on what Forrester sees as data security and privacy trends for 2019 to 2020:

› **Justify your budget by your investments' impact on security maturity and value.** The size of your budget says nothing about how well you spend those resources and whether your investments are lifting your security posture in a meaningful way. By assessing and measuring security maturity, S&R pros can better define and measure success.[16] Prioritizing investments based on security maturity returns will focus your investment in the right areas and at the right level of investment required. Building your business case on value will also provide a more balanced approach than solely focusing on potential breach costs.[17]

› **Explore emerging technologies and different approaches to data protection.** Consider these as complementary or supplemental — rather than a replacement — to your core controls to meet protection requirements for specific use cases. For example, look at technologies like homomorphic encryption to protect data-in-use, de-identification tools to facilitate sharing of data sets, or tools for persistent policy enforcement to support file collaboration.[18]

› **Focus on people to build a more robust security culture.** This includes considerations for prospective and current customers, as well as the board of directors, security staff, employees, and third-party partners and suppliers. Assess how your organization makes security and privacy relevant to different constituents, influencing security awareness and behavioral change.[19] This can help to reduce instances of inadvertent misuse of data as well as help constituents better understand rationale behind data security efforts.

› **Evaluate how your firm communicates about security and privacy.** Consider how you do this both through normal business operations as well as times of crisis like disruption to operations as well as data breach.[20] Include considerations for employee and customer communications in your breach response plans. For everyday communications relating to security and privacy, such as password resets or notifications to nudge customers to use two-factor authentication, ensure that how and what you communicate is tailored to your audience.

› **Build a culture that rewards whistleblowers and tighten your insider threat program.** Provide automated, anonymous ways for employees to communicate concerns to an independent third party as a way to protect employee privacy.[21] When developing or refining an insider threat program, recognize that it involves more than implementing technology capabilities for data loss prevention or employee monitoring. Account for employee experience and privacy in your approach.[22] This includes avoiding questionable practices (even if legal) and understanding employee privacy rights. Remember that insiders are not just employees but also your third-party partners that have access to your data and systems.

› **Develop a truly global privacy program, with a focus on sustained compliance.** GDPR-style regulation is here. The California Consumer Privacy Act of 2018 has now come into force, aligning to the standard of GDPR. Countries like Japan have agreed with the EU to evolve its domestic legislation to incorporate some GDPR requirements, while Brazil has adopted regulation very similar to GDPR. Work to embed elements of GDPR programs' governance into your broader privacy governance, data management lifecycle, and security strategy to ensure that you can respond in an agile manner to changing regulations around the globe.

Supplemental Material

Survey Methodology

The Forrester Analytics Global Business Technographics® Security Survey, 2019, was fielded from April to June 2019. This online survey included 3,890 respondents in Australia, Canada, China, France, Germany, India, the UK, and the US from companies with two or more employees.

The Forrester Analytics Global Business Technographics Security Survey, 2018, was fielded in May and June 2018. This online survey included 3,089 respondents in Australia, Canada, China, France, Germany, the UK, and the US from companies with two or more employees.

The Forrester Analytics Global Business Technographics Security Survey, 2017, was fielded in May and June 2017. This online survey included 3,752 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester's Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Dynata (2019) and ResearchNow (2018 and 2017) fielded these surveys on behalf of Forrester. Survey respondent incentives included points redeemable for gift certificates.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester's Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

Endnotes

[1] Source: Sarah Morgan, "Hershey accuses former health snack chief of trade secret theft," World IP Review, January 29, 2020 (https://www.worldipreview.com/news/hershey-accuses-former-health-snack-chief-of-trade-secret-theft-19252).

Source: Michelle Chipetine and Julia Milewski, "Scientist Pleads Guilty to $1 Billion in Trade Secret Theft," Trade Secrets Trends, November 15, 2019 (https://www.crowelltradesecretstrends.com/2019/11/scientist-pleads-guilty-to-1-billion-in-trade-secret-theft/).

Source: Sean O'Kane, "Former Tesla employee admits uploading Autopilot source code to his iCloud," The Verge, July 10, 2019 (https://www.theverge.com/2019/7/10/20689468/tesla-autopilot-trade-secret-theft-guangzhi-cao-xpeng-xiaopeng-motors-lawsuit-filing).

[2] Of the 25% of data breaches that security decision makers attributed to an internal incident, 48% said that abuse or malicious intent best characterized the incident. Base: 359 global security decision makers with network, data center, app security, or security ops responsibilities who experienced an internal incident within their organization that led to a data breach. Source: Forrester Analytics Global Business Technographics Security Survey, 2019.

When building an insider threat program, employee experience and privacy are critical considerations. For more information, see the Forrester report "Don't Poison Your Employee Experience With The Wrong Approach To Insider Threat."

[3] Base: 176 to 359 global security decision makers with network, data center, app security, or security ops responsibilities who experienced an internal incident within their organization that led to a data breach. Source: Forrester Analytics Global Business Technographics Security Surveys, 2018 and 2019.

[4] This report highlights some of the best communication and engagement methods that security leaders have used to instill a culture of security among executives, business and technology leaders, employees, and customers. For more information, see the Forrester report "Harden Your Human Firewall."

[5] Source: Forrester Analytics Global Business Technographics Security Surveys, 2018 and 2019.

[6] Fortunately, endpoint management and security tools are continuing to converge, with capabilities to improve threat prevention, detection, and response. For more information, see the Forrester report "The Forrester Wave™: Unified Endpoint Management, Q4 2019."

[7] In 2017, 41% of global decision makers said that PII had been breached in the past 12 months; this was 33% in 2018 and 37% in 2019, but in all three cases was the type of data most often mentioned as having been compromised. IP was mentioned by 29% in 2018, taking second place, and 33% in 2019, when it was mentioned third most often. Source: Forrester Analytics Global Business Technographics Security Surveys, 2017 to 2019.

[8] This Forrester Tech Tide™ report presents an analysis of the maturity and business value of 20 key technology categories that support data security and privacy. For more information, see the Forrester report "The Forrester Tech Tide™: Data Security And Privacy, Q3 2019."

[9] Security leaders should read this report to understand the practical building blocks of a successful Zero Trust implementation roadmap. For more information, see the Forrester report "A Practical Guide To A Zero Trust Implementation."

[10] This report details which encryption solutions are available to secure data in its various states and looks at the viability of emerging encryption technologies. For more information, see the Forrester report "Use Advanced Encryption For Data Security."

[11] For more information, see the Forrester report "Hybrid Cloud Security Best Practices."

[12] For more information, see the Forrester report "Tackle The California Consumer Privacy Act Now."

[13] For more information, see the Forrester report "Shift From Privacy Readiness To Sustained Compliance."

[14] For more information, see the Forrester report "CISOs, Get Ready To Pay More As Tech Titans Enter The Security Market."

[15] This report shows how each provider measures up and helps security and risk (S&R) professionals understand the respective strengths of each vendor's portfolio. For more information, see the Forrester report "The Forrester Wave™: Data Security Portfolio Vendors, Q2 2019."

[16] To help you build the business case for new projects and justify existing funding, the following report explains a unified way to plan, sequence, and explain the value of security investments based on their impact on your program's maturity. See the Forrester report "Justify Security Budget By Its Impact On Maturity."

[17] For more information, see the Forrester report "The Business Case For Data Security And Privacy."

[18] Recognize limitations of technologies as well. For example, de-identification isn't a bulletproof approach. For more information, see the Forrester report "Demystifying De-Identification, Anonymization, And Pseudonymization."

[19] CISOs can use this catalog of methods to move beyond online training courses and more effectively engage the hearts and minds of their key constituents. For more information, see the Forrester report "Harden Your Human Firewall."

[20] An upcoming Forrester report explores this topic in detail and will highlight examples of good response and a framework for thinking through your response strategy. Look for Forrester's upcoming report on breach response as an opportunity.

[21] Whistleblowers provide a mechanism for healthy corporate governance by exposing fraud and corruption and, more recently, revealing abusive practices, sexual harassment, discrimination, and privacy issues. This report outlines steps that risk pros must take to safeguard whistleblowers. For more information, see the Forrester report "Protect Whistleblowers For Business Success."

[22] Considerations for employees' privacy, company culture, and local standards for lawful, fair, and acceptable labor practices are key to the success of your insider threat program. For more information, see the Forrester report "Don't Poison Your Employee Experience With The Wrong Approach To Insider Threat."

FORRESTER®

forrester.com

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

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.