Don’t Poison Your Employee Experience With The Wrong Approach To Insider Threat

Security Leaders Must Balance Security, Governance, And Employee Privacy

by Joseph Blankenship and Enza Iannopollo

December 20, 2019

Why Read This Report

Your colleagues are one of the biggest threats to the security of your organization, but treating them as criminals is obviously not an option. 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. This report helps security and risk (S&R) pros set up a program that not only delivers against their security objectives, but doesn’t sacrifice employee experience (EX).

Key Takeaways

Insider Threat Programs Must Coexist With Employee Privacy Requirements
With the growing threat of insider-driven security incidents, many companies are creating rigorous insider threat programs, but security and risk leaders need to ensure these programs remain compatible with privacy regulations such as GDPR.

Employee Privacy Is A Strategic Component Of Robust Employee Experience
Forrester has linked positive employee experience to business outcomes such as higher levels of productivity and lower cost of talent acquisition. Be transparent about security with employees and respectful of their privacy.

Put People First To Advance Your Insider Threat Program
To develop an effective insider threat program, you must remember that insiders — employees, contractors, and partners — are people. And you need them to keep your business thriving. Putting people first humanizes your insider threat program while allowing it to be effective.

Don’t Poison Your Employee Experience With The Wrong Approach To Insider Threat

Security Leaders Must Balance Security, Governance, And Employee Privacy

by Joseph Blankenship and Enza Iannopollo
with Stephanie Balaouras, Elsa Pikulik, Madeline Cyr, and Peggy Dostie

December 20, 2019

Table Of Contents

Recommendations

Related Research Documents

Best Practices: Mitigating Insider Threats

The Five Milestones To GDPR Success

Recruiting And Retaining Insider Threat Analysts

FORRESTER®

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

A Poor Insider Threat Response Irks Employees And Invites Fines

With trusted access to your most sensitive data, insiders represent a real threat to your business. In 2015, malicious insiders accounted for 26% of our respondents' internal data breaches; in 2019, that rose to 48%.[1] Whether accidental or malicious, insider threat incidents can result in financial fraud, privacy abuses, intellectual property theft, or damage to infrastructure.[2] You must watch for suspicious behavior with a vigilant eye, especially given the level of privileged access trusted employees have to sensitive corporate and personal information. But, to be successful, your insider threat program must account for the growing protections for employee privacy, your company's culture, and local standards for the deployment of fair and acceptable labor practices.

Infringing Employee Privacy Will Result In A Hostile Work Environment . . .

The biggest risk when combating insider threat is cultivating an adversarial relationship with employees, turning your own colleagues into the enemy.[3] A poorly designed and executed insider threat program means you will lose your colleagues' trust. As a result, the business as a whole will suffer, because there is a direct link between employee experience and its impact on customer experience and overall business performance. Forrester has found that investment in improved employee experience leads to crucial benefits such as boosting productivity, conversion of brand advocacy into growth, and a reduction in talent acquisition, retention, and onboarding costs.[4] But a heavy-handed approach to insider threats:

- **Turns employees against their employers.** Fast-food chain Wendy's is facing a large class-action lawsuit in Illinois for alleged unlawful collection of employee fingerprint data. The suit filed in September 2018 centers on Wendy's use of biometric clocks to scan when employees are using point of sale systems as well as when they clock in and out. Employees claim that the company doesn't make it apparent how it uses this data and that it breaks the Illinois Biometrics Privacy Act.[5]

- **Undermines employees' expectation of care and protection and corporate culture.** Regulations such as GDPR make clear that employees are entitled to privacy rights, such as the right to be forgotten, data access, and portability.[6] Employers must also communicate clearly which data they want to collect, why, and for how long they intend to store or process it. But, even when requirements of this kind are not in place, S&R should not undermine their colleagues' expectations for care and protection. For example, the newly adopted California Consumer Privacy Act (CCPA) excludes employees from the protection offered to consumers. However, many S&R pros operating in that market are working to extend CCPA protection to their employees, too, because they expect it.

- **Demoralizes employees and undercuts their performance.** Employee success leads to customer satisfaction. Just as superior tech management strategies can lead to employee success, well-managed employee privacy strategies help reduce cost, with superior control and compliance. A study of more than 300 workers in both private and public sectors shows that poorly managed and communicated email monitoring policies not only damage workplace morale but also hurt the organization's profitability.[7] Lack of transparency also hinders employees' trust in their organization and increases levels of on-the-job paranoia.

› **Hampers the ability to recruit top talent.** Firms like Facebook and LinkedIn have adopted a data-driven approach to recruiting. Using data analytics, they can more accurately identify the best candidate for a position or check in on the wellbeing of their workforce. But collecting and analyzing the sensitive data of job candidates and employees, including their mental alertness and sugar levels, or even data from social media, creates serious privacy concerns that may discourage talented individuals from applying for or keeping a job.[8] In an attempt to mitigate these concerns, firms like Google publish candidate privacy notices on their websites, which explain in detail the conditions under which the firm uses job candidates' personal data.[9]

. . . But Neglecting Employee Privacy Will Result In Regulatory Fines

On the other hand, inaction or lassitude in monitoring insider threats can lead to potential privacy abuses, class actions, and other lawsuits. The regulatory fines that follow will definitely kill your program and maybe cost you your job. A half-hearted approach to insider threats:

› **Exposes the firm to significant regulatory fines.** On May 25, 2018, European regulators started enforcing the EU General Data Protection Regulation (GDPR) and its stringent requirements. S&R pros should be aware that employees, not just consumers, benefit from the privacy rights included in the GDPR (see Figure 1).[10] The definition of personal identifiable information that falls within the scope of the law is broader than many S&R pros suspect, and they must define a workable list (see Figure 2). They must also consider the legal implications of transferring their employees' personal data across geographies. Before program implementation, they should discuss with their vendors of choice whether frameworks such as privacy shield or binding corporate rules (BCRs) are necessary and available to them.

› **Breaches local requirements of legal, fair, and acceptable practices in the workplace.** While GDPR enforcement will become more harmonized over time, some differences in the implementation of the rules remain. For example, if you plan to track data relating to medical or racial status of the workforce in France, you must get the local Data Protection Authority (DPA)'s prior written approval. In the UK, consent for monitoring can be part of the employment contract, but this is a dealbreaker in Germany. Also, labor councils' standards and labor laws demand a local focus. Our interviews revealed that overcoming labor councils' concerns can be incredibly difficult. Not only are there large variations in the rules and practices at the national level, but labor councils at each firm have different levels of tolerance for tools that allow the monitoring of employees.

FIGURE 1 Employee Rights Under Privacy Regulations

Employee rights under privacy regulations
The right to be informed, which requires employers to provide transparency as to how they will use personal data
The right to access the data you hold on them
The right to rectify data that is inaccurate or incomplete
The right to be forgotten under certain circumstances
The right to block or suppress processing of personal data
The right to data portability, which allows employees to obtain and reuse their personal data for their own purposes across different services under certain circumstances

FIGURE 2 Employee Privacy Includes A Wide Range Of Data Types

Examples of employee personal data types
Annual appraisal/assessment records
Annual leave records
Application forms and work references
Attendance records
Disciplinary matters
Information generated by computer systems
Internet access
Location data
Payroll and tax information/tax and social benefits information
Personal email use data
Pictures
Records relating to promoting, transfer, training
Reimbursement of expenses, e.g., travel
Sickness records
Unpaid leave/special leave records
Videos

Win Over Employees With Transparency And Respectful Protocols

A successful insider threat program makes employees a valuable part of it. Winning the hearts and minds of your insiders requires open and transparent communication about the nature of your program, why it exists, and how employees fit into it. To rally employees to your cause, you must:

- **Communicate the program and related IT policies openly.** Don’t make the insider threat program a secret. Let the employees know you’re watching. Tell them about the technologies that you will use, and explain how they work and how you will handle the process to ensure minimal privacy intrusion. Clear IT policies about private use of corporate infrastructure are also useful to determine your action plan. For example, in Germany, if an employer forbids employees from using the internet to check social network accounts, it’s easier to justify the need for monitoring. Where IT policies are more relaxed, you must think more carefully about the legal basis that will enable you to lawfully collect and process your employees’ data.

- **Be crystal clear when defining the objectives of your program.** You can’t use employee monitoring to satisfy goals outside the stated goals of the program. From performance evaluation, to engagement metrics, to security, there is no shortage of reasons why knowing more about employees’ actions might be interesting. If you do it for security, be clear about it. And, it’s not just an issue of transparency. The legal requirements that apply in the context of ensuring corporate security are different than those applying to other activities. For example, labor councils and data protection officers might be more open to allow an insider threat program as a “legitimate interest” of the firm, while requiring explicit consent for other types of monitoring.

- **Let employees know they’re part of the security team.** In the theme of “If you see something, say something,” encourage your users to make anonymous tips about suspicious behavior they’ve observed. For example, Apple employees recognized a colleague’s unusual behavior when they saw him taking pictures of his workspace and reported it to security. The alleged insider was found with “over two thousand files containing confidential and proprietary Apple material, including manuals, schematics, and diagrams” and was subsequently arrested by the FBI.[11] Be careful with the language you choose; the word “report” often has a negative connotation to users. Take the opportunity to educate them at the same time. Users are the last line of defense for security. The decisions they make will directly impact the success or failure of a phishing scheme or social engineering attempt.

- **Make your insider threat program fit within the overall security program.** Among regulators, as well as users, there is growing awareness that the security of your organization is a priority. For example, the GDPR itself contains remarks about the need of processing personal data to ensure the security of networks, systems, etc.[12] For these practices to be allowed, S&R must make sure that their employees’ data collection and processing activities are strictly necessary and that their purpose is proportionate to the overall goal that they want to achieve. A well-documented security posture will provide the perfect starting point. The less risk appetite for security threats, the easier it will be for you to demonstrate that your measures are proportionate and legitimate.

- **Follow traditional security best practices when deploying the program.** When deploying the program, traditional best practices apply: S&R pros must ensure that no one person in the organization has full access to all files. Admins must have limited access to data, and their own user accounts must be separate from administrator accounts. Some vendors provide the capability to completely anonymize private employee data or limit the administrator’s access to sensitive information. And, you must ensure that only when there is evidence of suspicious behavior, and with specific approval, is any identifiable information disclosed as part of the investigation (see Figure 3). Finally, the employment contracts of staff that access that data should also include a professional secrecy clause.

› **Don't let security become a burden on employee productivity.** If your security policies create a lot of friction between your employees and the work they need to accomplish, then they are more likely to break protocol. In fact, 9% of global information workers said that security software reduces their work productivity, while 7% said they sometimes ignore or go around security policies, offering a variety of reasons for doing so (see Figure 4).[13] When employees break protocol, they're more likely to inadvertently breach data. Among our survey respondents, accidents make up 43% of insider-related data breaches.[14] Make sure you have secure and easy authentication processes like single sign-on (SSO) and that your two-factor authentication (2FA) practices are frictionless for users.

FIGURE 3 Obfuscate Employee Identity Until Starting An Investigation

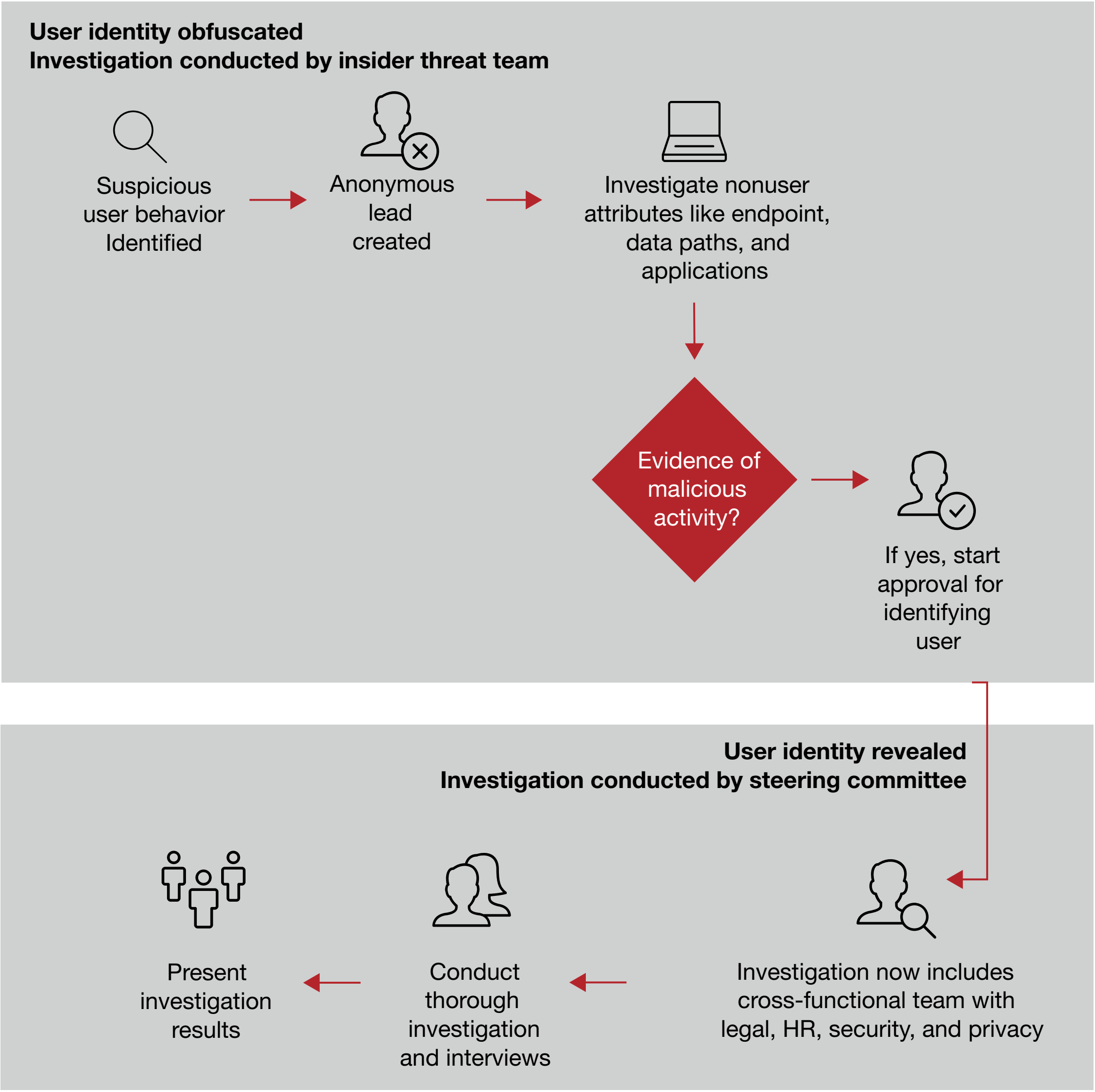
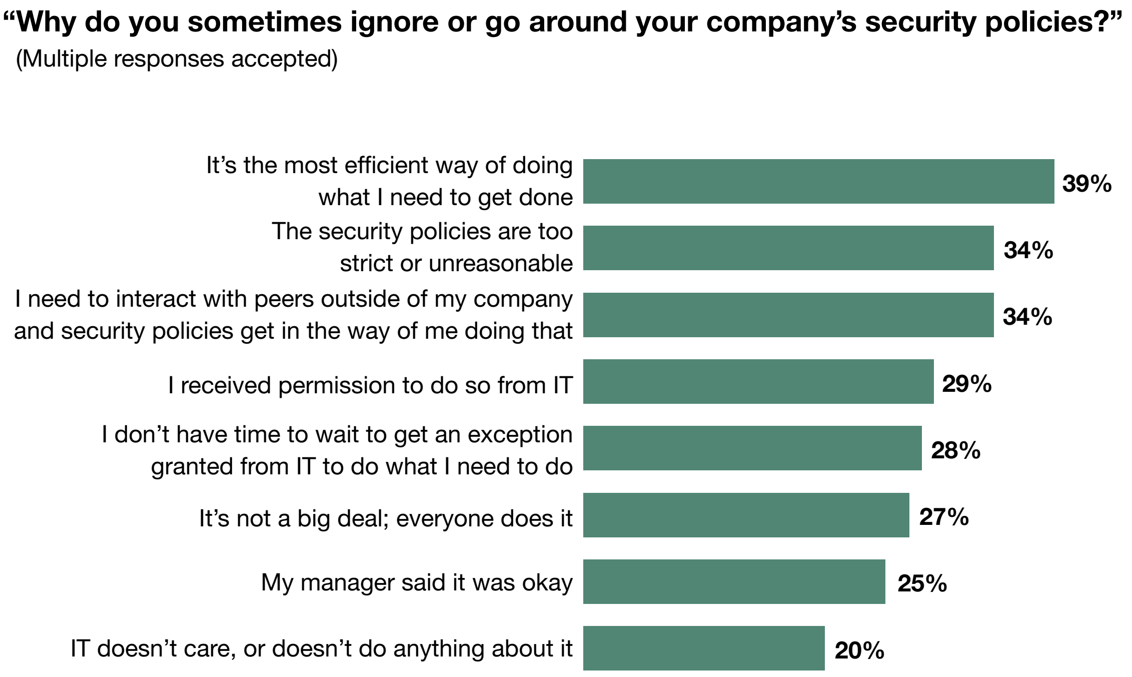

User identity obfuscated
Investigation conducted by insider threat team
Suspicious user behavior Identified
Anonymous lead created
Investigate nonuser attributes like endpoint, data paths, and applications
Evidence of malicious activity?
If yes, start approval for identifying user
User identity revealed
Investigation conducted by steering committee
Investigation now includes cross-functional team with legal, HR, security, and privacy
Conduct thorough investigation and interviews
Present investigation results

FIGURE 4 Information Workers Offer A Variety Of Reasons For Ignoring Or Circumventing Security Policies



Base: 519 global information workers who sometimes ignore or go around their company’s security policies

Source: Forrester Analytics Global Business Technographics® Workforce Benchmark Recontact Survey, 2019

Technology And Human Intelligence Fuel Your Insider Threat Program

After you ensure you are respecting privacy, have educated your employees, and are compliant with all laws, it’s time to establish your insider threat hunting program. Detecting malicious insiders requires a defined process and a focused team in addition to detection technologies. You must:

- **Enable process with technology, outsourcing, and training.** Choose the technology tools that best fit your needs. Security user behavior analysis (SUBA) solutions like those from Bay Dynamics, Exabeam, Forcepoint, Gurucul, Interset (Micro Focus), and Securonix detect suspicious user activity. Solutions from companies like Digital Guardian, Dtex Systems, ObserveIT (Proofpoint), and Varonis monitor user interactions with data to detect risky behavior. Vendor Code42 takes the focus off users and instead focuses on file behavior. Service providers like Accenture, Aon, BAH, Deloitte, EY, Leidos, PwC, and Rapid7 can provide guidance to establish the insider threat program. The CERT Insider Threat Center offers training and certification for insider threat teams and managers.[15]

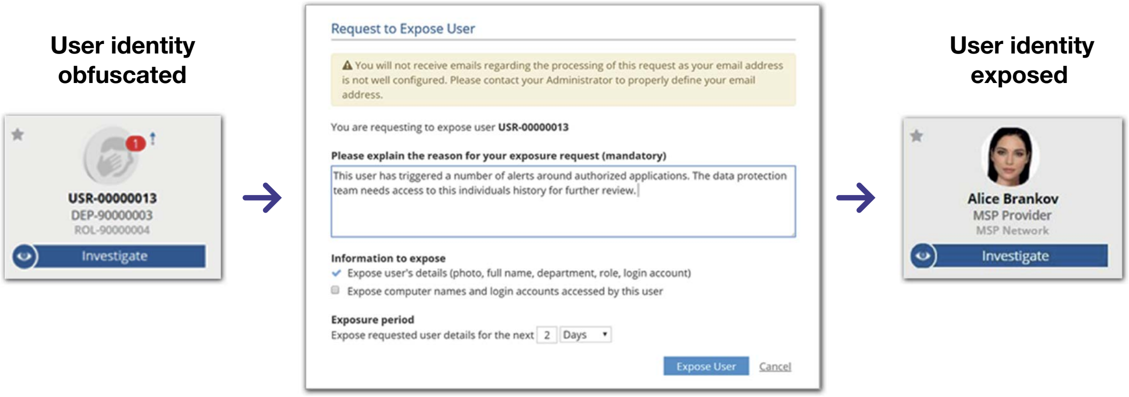
- **Create a cross-functional team.** Your insider threat program needs to work across the organization. Executives from the top down must buy into the program, including the CEO and the board. Functions like internal audit, risk, privacy, and the CIO should be part of your support organization. Managers, coworkers, and HR professionals have insights into insiders and their behavior beyond what security teams can monitor. If you decide to prosecute, having relationships with local law enforcement or the FBI beforehand will be helpful.

- **Understand your employees and monitor for suspicious work behavior.** For example, you need to understand what systems your sales force uses on a regular basis and what their typical download sizes are. In some contexts, there is high value in understanding where your employees are; if you have users entering and exiting high-risk areas, it may be necessary to use badging and surveillance logs for forensic reasons. Respect employee privacy. Technology solutions should obfuscate employee identities until the decision has been made to start an investigation. Insider threat analysts shouldn’t discuss employees outside of the insider threat team.

- **Understand your employees and monitor for suspicious personal behavior.** Financial distress, revenge, work conflicts, ideology, nation-state influence, fear of layoffs, etc. are common motivations for disgruntled employees. While acting within your employee privacy policy, you need to keep an eye on these behaviors. (see Figure 5). However, be conscious of what data you collect on employees. For instance, in some jurisdictions it could be fine to collect data on employee credit scores, but in others it is illegal.[16] Also be cautious of monitoring employee social media for signs of trouble. Some labor councils and employees themselves might label this approach as unethical, and too much monitoring could lead to eroded employee trust.[17]

- **Treat every investigation as if it will end up in court.** After you’ve made the decision to start an investigation, proceed as if you’re entering a legal investigation. Even if you decide not to prosecute, having evidence that you followed the process will help you if an employee decides to sue. If you fail to enforce policies consistently, employees and their legal teams can challenge the investigation in court. This is another reason for having an updated acceptable use policy.

Figure 5 Obfuscated Versus Exposed User Identity



Request to Expose User

⚠ You will not receive emails regarding the processing of this request as your email address is not well configured. Please contact your Administrator to properly define your email address.

You are requesting to expose user **USR-00000013**

Please explain the reason for your exposure request (mandatory)

This user has triggered a number of alerts around authorized applications. The data protection team needs access to this individuals history for further review.

Information to expose

✓ Expose user’s details (photo, full name, department, role, login account)
□ Expose computer names and login accounts accessed by this user

Exposure period

Expose requested user details for the next 2 Days ▾

Expose User Cancel

Recommendations

Differentiate EX By Prioritizing Employee Privacy And Security Culture

Highly visible perks such as open office plans, free food, and drinks can be expensive and may not have the desired ROI for employee experience. Companies should craft their benefits to reflect what really matters to employees: feeling empowered, inspired, and appreciated to enhance their productivity.[18] When you take a transparent and respectful approach to insider threat programs, employees will understand that the organization and the security team value their privacy and they will feel respected by their employer. To further this mission:

- **Regard employees as a special type of protected party.** Employee privacy is the next privacy battleground. Organizations that don’t respect privacy as part of both their CX and EX efforts will demoralize employees and sabotage the company’s ability to recruit top talent. After the Cambridge Analytica Scandal, the full-time work-offer acceptance rate among new graduates dramatically declined at Facebook.[19]
- **Make security culture company culture.** For a successful insider threat program, you must have security champions distributed throughout the organization. Promoting security culture is crucial for disseminating security procedures and policies throughout the organization. Be proactive: Don’t wait for a breach to be continuously maintaining. advocacy and visibility for security across the organization.

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

Survey Methodology

The Forrester Analytics Global Business Technographics® Workforce Benchmark Recontact Survey, 2019, was fielded in July and August 2019. This online survey included 7,388 respondents in Australia, Canada, China, France, Germany, India, the UK, and the US from companies with two or more employees who had already participated in our Global Workforce Benchmark Survey, 2019.

Forrester Analytics’ Business Technographics ensures that the final survey population only includes information workers who use a connected device for work at least 1 hour per day. Dynata fielded this survey 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 Analytics’ Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time

Endnotes

[1] Source: Forrester Analytics Global Business Technographics Security Surveys, 2015 and 2019.

[2] Whether accidental or malicious, insider incidents can result in financial fraud, privacy abuses, intellectual property theft, or damage to infrastructure. It’s difficult for security pros to detect this suspicious activity because insiders need to have privileged access to data to do their jobs. Since insiders are people and, therefore, entitled to privacy and due process, security pros must handle these incidents with greater care than external threats. This report describes how to build an insider threat program. See the Forrester report “Best Practices: Mitigating Insider Threats.”

[3] See the Forrester report “Protect Your Intellectual Property And Customer Data From Theft And Abuse.”

[4] EX is becoming ever more important due to an increasingly educated workforce, incredibly low unemployment rates, pervasive AI/automation, and workplaces beset by multiple transformation initiatives. But many executives see a superior EX as an important, but unquantifiable, nice to have. We believe that EX ROI is quantifiable and that EX investments will manifest in unexpectedly large returns — and from areas overlooked by C-level executives. This report will help EX practitioners make a strong business case for EX by using Forrester’s Total Economic Impact™ (TEI) methodology. See the Forrester report “The ROI Of EX.”

[5] Source: Catalin Cimpanu, “Wendy’s faces lawsuit for unlawfully collecting employee fingerprints,” ZDNet, September 23, 2018 (https://www.zdnet.com/article/wendys-faces-lawsuit-for-unlawfully-collecting-employee-fingerprints/).

[6] Not all rights apply equally and automatically. Some rights, such as the right to be forgotten, applies when data is collected through consent. Other rights apply more broadly. Firms must define which rights apply to which data and define retention policies to ensure they can handle employees’ requests.

[7] Source: Matt Palmquist, “How E-mail Privacy Affects Morale,” strategy+business, November 23, 2010 (http://www.strategy-business.com/article/10411b?gko=5d277).

[8] Source: John Burn-Murdoch, “Is the recruitment industry set for a big data revolution?” The Guardian, August 8, 2013 (http://www.theguardian.com/news/datablog/2013/aug/08/recruitment-industry-set-for-big-data-revolution).

[9] Source: “Applicant and Candidate Privacy Policy,” Google Careers, August 23, 2019 (https://careers.google.com/privacy-policy/).

[10] Source: Judith Nink, “How will GDPR affect employee data?” GDPR press release, May 29, 2018 (https://gdpr.report/news/2018/05/29/how-will-gdpr-affect-employee-data/).

[11] Source: Sean O’Kane, “A second Apple employee was charged with stealing self-driving car project secrets,” The Verge, January 30, 2019 (https://www.theverge.com/2019/1/30/18203718/apple-self-driving-trade-secrets-china-titan?utm_campaign=theverge&utm_content=chorus&utm_medium=social&utm_source=twitter).

[12] Source: Recital 49 EU GDPR, SecureDataService (http://www.privacy-regulation.eu/en/recital-49-GDPR.htm).

[13] Source: Forrester Analytics Global Business Technographics Workforce Benchmark Recontact Survey, 2019.

[14] Source: Forrester Analytics Global Business Technographics Security Survey, 2019.

[15] Whether accidental or malicious, insider incidents can result in financial fraud, privacy abuses, intellectual property theft, or damage to infrastructure. It’s difficult for security pros to detect this suspicious activity because insiders need to have privileged access to data to do their jobs. Since insiders are people and, therefore, entitled to privacy and due process, security pros must handle these incidents with greater care than external threats. See the Forrester report “Best Practices: Mitigating Insider Threats.”

[16] Source: Susan Ladika, “Employer credit checks: Who does them, how they work and what laws apply,” CreditCards.com, January 15, 2019 (https://www.creditcards.com/credit-card-news/employer-job-credit-report-check-1270.php).

[17] Source: “Monitoring Employee Social Media Activity at Work,” The Hartford (https://www.thehartford.com/business-playbook/in-depth/employee-social-media-monitoring).

[18] See the Forrester report “The ROI Of EX.”

[19] Facebook’s acceptance rate for full-time positions offered to new graduates has fallen from an average of 85% for the 2017-2018 school year to between 35% and 55% as of December, according to former Facebook recruiters. Source: Mark Sweney, “Facebook job offers ‘shunned by top talent after data scandal,’” The Guardian, May 17, 2019 (https://www.theguardian.com/technology/2019/may/17/facebook-job-offers-shunned-by-top-talent-after-cambridge-analytica-scandal-report).

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.