Establish The People And Culture Foundation For Cybersecurity And Privacy Excellence

Beginner Level: People Practices For Cybersecurity And Privacy

by Enza Iannopollo

September 25, 2018

Why Read This Report

If you're just starting your journey to cybersecurity and privacy maturity, you're not alone. If CIOs, chief information security officers (CISOs), and chief privacy officers (CPOs) establish strong repeatable practices, they can progress quickly. This report — the first of three in the people competency of the cybersecurity and privacy playbook — helps CIOs meet the challenges of the beginner phase.

Key Takeaways

Focus On Four Key Aspects Of Cybersecurity "People And Culture"
These are: 1) proactive external communication; 2) organizational alignment; 3) cybersecurity and privacy culture for the workforce; and 4) skills management for cybersecurity and privacy staff.

Use Required Policies And Communications To Drive Customer Trust
Every public-facing cybersecurity or privacy policy is an opportunity to show customers that you will put them first.

FOR CIOS

Establish The People And Culture Foundation For Cybersecurity And Privacy Excellence

Beginner Level: People Practices For Cybersecurity And Privacy

by Enza Iannopollo
with Laura Koetzle, Stephanie Balaouras, Nick Hayes, Claire O'Malley, Heidi Shey,
Elsa Pikulik, and Rachel Birrell

September 25, 2018

Table Of Contents

Related Research Documents

Best Practices: Recruiting And Retaining Women In Cybersecurity

Harden Your Human Firewall

Maintain Your Security Edge

FORRESTER®

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

Tune Your Human Firewall: Cybersecurity And Privacy Rely On People

Your people determine your cybersecurity and privacy culture — and here we mean not just the individuals in your CISO's and CPO's teams who build, oversee, and maintain your security and privacy programs but your entire workforce. To quickly zero in on the people and culture side of your cybersecurity and privacy journey, complete the assessment tool for this cybersecurity and privacy playbook.

Prerequisite: Establish Repeatable Procedures

If you find that your firm either doesn't follow the practices we ask about in the assessment or doesn't follow them consistently, don't despair. You're not the only CIO in this position. By focusing on the right areas, you and your team can make progress quickly.

- **Establish routine practices that respect and protect data.** Employee errors remain the most common cause of data breaches. Repeatable practices can help you catch those mistakes and mitigate their damage. To create strong routines, look for good, simple, ad hoc practices; reward them; and formalize them. Explicitly link those routines to protecting brand and reputation. For example, don't just tell employees to lock their devices when they leave their desks. Instead, explain, "You have access to our customers' personal data. Think about your colleague at your electricity provider. Would you want your home address to be visible to anyone who walked by his desk while he was at lunch?"

- **Identify the level of cybersecurity and privacy expertise that employees need.** Employees who only handle pseudonymized or encrypted data (low risk) require less cybersecurity and privacy savvy than do the researchers working on your next blockbuster drug or the team vetting your next acquisition target (both high risk). Work with your cybersecurity and privacy leaders to sensibly define the risk level and required expertise.

- **Define a plan to communicate about cybersecurity and privacy to your customers.** Today, customers and partners evaluate your cybersecurity and privacy practices alongside your products and services. Increasingly, consumers know their rights and actively use them; For example, 62% of UK online adults reported that they are likely to ask companies to delete their data, and 62% said that they are likely to ask companies not to profile them for marketing purposes.[1] And it's not just in Europe: The recent California Consumer Privacy Act contains similar provisions.[2] Even if your privacy program is small today, define and communicate what you must share with your customers and be ready to update it continuously.[3]

For Beginners And Beyond: Understand Where You Are In Your Organizational Journey

Once you've established those repeatable practices, you're ready for your next steps. Refer to your assessment results, which cover three phases of maturity across four key "people and culture" areas: 1) proactive external communication; 2) organizational alignment; 3) cybersecurity and privacy culture for the workforce; and 4) skills management for cybersecurity and privacy staff (see Figure 1). Here's what your level means:

- **Beginner organizations master the basics.** These firms have some of the fundamentals of policy, training, good hygiene, and communication in place, and they are working to define and institute them all. They remain primarily compliance driven but are beginning to embrace cybersecurity and privacy elements as part of their culture.
- **Intermediate organizations apply baseline metrics.** In this stage of the journey, you start to measure everything. Your cybersecurity and privacy teams are creating baseline metrics to track growth over time. These metrics build on the policy foundations of the beginner phase, and they span topics from customer data to third-party risk to hiring.
- **Advanced organizations enhance their organization's reputation via best practices.** They adapt rapidly to changes and optimize their activities continuously. They strive to establish best practices and build best-in-class organizations. These firms treat cybersecurity and privacy as core values; invest in talent; promote diversity; and incentivize continuous collaboration between security and privacy experts and the rest of the organization. They aim to differentiate their firms in the eyes of customers and partners with excellent cybersecurity and privacy practices.[4]

FIGURE 1 The Beginner Stage Establishes Privacy Best Practices And Training

People and culture domain	Beginner	Intermediate	Advanced
Proactive, external communication	• Publish a privacy policy (including mechanisms for requesting personal data). • Publish a cookie policy. • Provide users with password creation guidance. • Include cybersecurity and privacy in messaging to customers and partners.	• Measure the frequency of the updates to the privacy policy. • Measure customer opt-in and data subject right requests.	• Automate processes to trigger privacy policy updates when new data collection/processing activities are planned. • Map consent and privacy policies to customer journeys and update them continuously. • Offer a “defined experience” for data subject right requests and automate the underlying processes so they allow for scale.
Organizational alignment (roles/ responsibilities)	• Provide guidance for procurement on cybersecurity and privacy requirements for third parties. • Get input from stakeholders into policies.	• Review exception rates to cybersecurity and privacy policies. • Build a cross-functional privacy committee. • Build a cross-functional information risk team. • Establish cybersecurity and privacy champions in functional and geographic units and measure effectiveness. • Include privacy standards in third-party risk assessments and measure them on an ongoing basis.	• Set a goal for the head of privacy and a business unit head to jointly lead key initiatives that involve personal data collection/processing (e.g., the CPO and the CMO jointly lead a specific marketing campaign). • Follow a process for approving high-risk initiatives where the CPO and CISO are key decision makers.

FIGURE 1 The Beginner Stage Establishes Privacy Best Practices And Training (Cont.)

People and culture domain	Beginner	Intermediate	Advanced
Cybersecurity and privacy culture (includes security and privacy baseline skills for all employees)	• Verify that teams run regular cybersecurity and privacy training and awareness programs at defined points in employee development (onboarding, new responsibilities), including role-specific training (e.g., security skills for app developers). • Provide and consistently require targeted (risk-based) training for high-risk roles. • Include physical reminders of cybersecurity and privacy in physical workspaces (posters, etc.).	• Measure the effectiveness of cybersecurity and privacy training programs and refine them over time. • Ensure that your CISO and CPO identify and capture best/worst practices for everyday activities for specific roles.	• Produce a continuous, year-long “cybersecurity and privacy curriculum” for all employees (independent of employee life-cycle events). • Run regular programs where employees regularly discuss best/worst practices.

FIGURE 1 The Beginner Stage Establishes Privacy Best Practices And Training (Cont.)

People and culture domain	Beginner	Intermediate	Advanced
Skills management for cybersecurity and privacy staff (training, recruiting/ retention)	• Ensure training for data protection officers (DPOs). • Promote attendance at relevant conferences. • Encourage certification attainment (CISSP, CIPP, etc.). • Have a firm statement on valuing workforce diversity.	• Establish a methodology for measuring the thought leadership of your CISO and CPO. • Work with HR to build recruitment pipelines for nontraditional candidates to get more talent into cybersecurity and privacy. • Ensure that the CISO and CPO work with HR to lay out clear, documented employee career development paths for cybersecurity and privacy people. • Create defined and measurable policy goals for recruiting, promoting, training, and retaining a diverse cybersecurity and privacy workforce.	• Achieve high scores for thought leadership using your metrics for the CISO and CPO, who are known as leaders in their fields. • Formalize a partnership with HR (regular meetings to discuss relevant skills, emphasizing unteachable qualities/potential as well as technical certifications). • Be recognized for recruiting, developing, and promoting a diverse workforce from both traditional and nontraditional cybersecurity and privacy backgrounds.

Use Policies And Standards To Encourage Competency Building

Help your CISO and CPO harness compliance mandates to catalyze culture change. Policies and standards exist to meet your regulatory objectives and protect data. But you can also use them to educate employees about good behaviors and practices and the value that these deliver to internal stakeholders and customers. To advance to the next level of maturity:

› **Publish privacy notices that promote customer engagement and trust.** Attorneys and privacy and security experts craft privacy policies and consent notices to fulfill regulatory obligations. But these documents are also an opportunity to engage your customers and stimulate trust in the organization. Build a process that promotes collaboration with customer experience and customer insights pros to make sure that your external communication takes an outside-in approach, integrates well with existing customer journeys, and accounts for customers' privacy attitude and behaviors.

- **Adopt a cross-functional approach to designing and executing policies and standards.** Beginner firms must eliminate the disconnects between policy creation, implementation, and enforcement. From managing third-party risk to defining data retention policies for marketing or HR purposes, you as CIO can build the bridges your team needs to collaborate effectively across functions and departments.

- **Drive continuous education.** Even at beginner firms, sporadic training and awareness campaigns don't work. Instead, ensure that your cybersecurity and privacy teams offer training to support all transitions, such as when an employee becomes a manager. In addition to risk-based training — HR staff who handle sensitive employee data need different training than economists who work with aggregate data — your colleagues need job-specific security and privacy help, such as secure coding skills for developers.

- **Build and diversify your cyberprivacy and security team portfolio.** CIOs must send their cybersecurity and privacy experts to conferences, forums, courses, and certification programs to promote continuous skill development. Unless you're lucky enough to be based in a major tech hub and have deep pockets, your CISO and CPO are doubtless having trouble finding staff. Help them broaden their recruitment efforts beyond the usual sources to build a diverse, high-performing team.[5]

Recommendations

Shift Focus From Compliance To Core Values To Drive Maturity

While the efforts of beginner firms are primarily driven by compliance, this is the stage when corporate culture starts to embrace cybersecurity and privacy as core values. CIOs at beginner firms must advance the development of their cybersecurity and privacy culture, engaging in a mix of both externally and internally focused initiatives. Specifically, they must:

- **Map customer journeys to align policies and third-party requirements.** Now that you have decided what to communicate to your customer and how, make sure that: 1) you assess how it impacts customer interactions and the overall experience and 2) it aligns with broader cybersecurity and privacy policies, including those for third parties. Choose a customer journey that requires a customer to read your privacy notices and involves third-party data sharing, and then map it. This exercise will uncover when and how the ecosystem touches personal data and ensure the consistency and suitability of your policies.

- **Build a privacy-by-design framework to promote collaboration.** According to the principle of privacy by design, the assessment and mitigation of privacy risks must be a core part of any project that touches on personal data. This means that, regardless of the business unit owning the project, cross-functional collaboration must occur regularly to recognize and remediate these risks. Build a process to enable this collaboration and promote awareness. For example, have your app development team co-create a privacy and security assessment with their security and privacy peers. Ensure that as they begin a new project, the app developers compile the assessment and run a face-to-face review with their security peers to determine the best remediation strategy moving forward.

› **Innovate on cybersecurity and privacy education.** Don’t stop at traditional training methods when educating your workforce. Complement your desktop-based class with informational posters and flyers around the office. Make them as memorable as possible by using humor, and make them as relevant as possible to employees’ daily activities or to a new broader company campaign. In addition, create collateral like podcast and videos that employees can consume on demand and that explains why they should adopt certain behaviors. Experiment with interactive interfaces and dedicated apps with features like games and quizzes.[6]

Endnotes

[1] Source: Forrester Analytics Consumer Technographics® European Online Benchmark Survey (Part 2), 2018.

[2] The General Data Protection Regulation (GDPR) has changed how B2C marketers and advertisers operate in the European Union (EU). But more privacy regulations are on the horizon, from the US to Japan, all of which will require marketers to take procedural and technical steps to protect consumers and show more transparency in their data practices. See the Forrester report "Marketing Under GDPR Hinges On Data Governance."

[3] Forrester uses its Consumer Privacy Segmentation and Empowered Customer Segmentation to understand how privacy perspectives vary by geography and type of regulations in the EU-5. B2C marketers should use this information to understand their consumers and build trust. See the Forrester report "Introducing Forrester's Consumer Privacy Segmentation — EU" and September 28, 2017, "Understand Forrester's Privacy Segments In Europe To Please Your Customers Without Upsetting The Regulators" Webinar (https://www.forrester.com/webinar/Understand+Forresters+Privacy+Segments+In+Europe+To+Please+Your+Customers+Without+Upsetting+The+Regulators/-/E-WEB23786).

[4] Data is the lifeblood of today's 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 unnecessary privacy abuses can bring unwanted scrutiny and regulatory fines while damaging reputations. Security and privacy pros must ensure 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."

[5] New security objectives and approaches call for shifts in architecture and operations — and, more importantly, for security leaders to reassess their investments in their most valuable asset: employees. Complacency, a widening gap between skills and talent, and a focus on technologies over people are a threat to the business. In an environment of competitive hiring and fast-evolving threats, security and risk leaders must invest in professional development and growth for themselves and their staffs. See the Forrester report "Maintain Your Security Edge."

[6] Human mistakes can render even the most sophisticated technical security controls useless. However, you can reduce the inherent vulnerability of your workforce and even turn staff into a strong security asset. This requires more than just training and awareness; your focus should be on effecting behavioral change. Forrester shares lessons from CISOs, training firms, and communications experts to describe an approach to reducing security risks with your firm's employees. See the Forrester report "Harden Your Human Firewall."

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.

Forrester Research (Nasdaq: FORR) is one of the most influential research and advisory firms in the world. We work with business and technology leaders to develop customer-obsessed strategies that drive growth. Through proprietary research, data, custom consulting, exclusive executive peer groups, and events, the Forrester experience is about a singular and powerful purpose: to challenge the thinking of our clients to help them lead change in their organizations. For more information, visit forrester.com.