Lay Your Security Tech Foundation

Beginner Level: Technology Practices For Cybersecurity And Privacy

by Stephanie Balaouras, Amy DeMartine, and Jeff Pollard

September 25, 2018

Why Read This Report

This report — the first of three in the technology competency of the cybersecurity and privacy playbook — outlines the technologies that CIOs and other technology leaders should prioritize to move to a data-centric Zero Trust security strategy. This strategy establishes the foundation your firm needs to mature its cybersecurity and privacy efforts, focusing on four key areas: 1) data governance; 2) data security; 3) cloud governance; and 4) technology innovation.

Key Takeaways

Start By Gaining Situational Awareness
Most firms starting or restarting their cybersecurity and privacy efforts will struggle with knowing what they have and where it goes. Thus, look first at your data security, platforms, independent governance tools, and privacy technologies.

Achieve Compliance To Gain Customer Trust
Don't fall into the trap of securing everything evenly. The workloads and applications your customers depend on are moving to the cloud. To preserve customer data and trust, differentiate your protection of those applications.

Lay Your Security Tech Foundation

Beginner Level: Technology Practices For Cybersecurity And Privacy

by Stephanie Balaouras, Amy DeMartine, and Jeff Pollard
with Laura Koetzle, Enza Iannopollo, Heidi Shey, Elsa Pikulik, and Peggy Dostie

September 25, 2018

Table Of Contents

Related Research Documents

Assess Your Cybersecurity And Privacy Maturity

The Future Of Cybersecurity And Privacy: Defeat The Data Economy's Demons

The Strategy Handbook: How CIOs Can Drive Security And Privacy Improvement

FORRESTER®

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

Establish A Cybersecurity And Privacy Foundation For Customer Trust

Today, savvy customers worry about their privacy and a business' ability to protect them from cybercriminals, fraudsters, dubious third parties (e.g., Cambridge Analytica), and government surveillance. If your results from the technology section of the assessment tool in this playbook place you in the beginner level, don't despair — you're not alone.[1] At this early stage of the cybersecurity and privacy journey, CIOs must work with their information security and privacy leaders to lay the technology foundation for securing the business and protecting the brand. This foundation will help you build customer trust and drive competitive differentiation with cybersecurity and privacy.

Four Technology Areas Are Essential To Cybersecurity And Privacy

At the beginner level, you must invest in technologies that help to: 1) establish basic data governance, achieve compliance, and protect employees and customers from the most egregious privacy abuses; 2) begin your Zero Trust security transformation; 3) reduce the inherent risks in cloud adoption; and 4) ensure the organization has the appropriate risk management and ethical guardrails in place to embed basic cybersecurity and privacy considerations in innovation. These technologies span the four critical areas that we emphasize in the assessment — data governance, data security, cloud governance, and technology innovation (see Figure 1).

FIGURE 1 Focus On Four Technology Areas To Drive Cybersecurity And Privacy

Key technologies	Beginner	Intermediate	Advanced
Data governance • Data discovery and flow mapping • Data classification • Data access governance • Data management platform • Data archiving • Data encryption • Secure file sharing and collaboration • eDiscovery • Consent/data subject rights management • Data privacy/GDPR compliance management • Breach notification • User behavior monitoring	**Strategy:** Achieve essential regulatory compliance and reduce the costs of investigations, lawsuits, and third-party audits. **Technology priorities:** • Develop core capabilities to inventory, map, and classify sensitive data. • Adopt solutions to continuously track personal data. • Encrypt sensitive data by default. • Use software to assess compliance posture and operationalize workflows. • Implement archiving and eDiscovery solutions.	**Strategy:** Proactively protect customers and employees from privacy abuses and other violations. **Technology priorities:** • Streamline and automate privacy management workflows. • Continuously maintain data inventory and visualization of data flow mapping. • Continuously map user access and behavior and automate customer data controls. • Aggressively archive and defensibly delete data. • Detect and respond to breaches within 72 hours with automation and orchestration.	**Strategy:** Differentiate the brand and drive growth with customer trust. **Technology priorities:** • Use data intelligence to improve CX. • Support data monetization and personalization with anonymization efforts. • Link data flows with customer journey to embed data governance. • Manage your broader third-party ecosystem and data flow dependencies.

FIGURE 1 Focus On Four Technology Areas To Drive Cybersecurity And Privacy (Cont.)

Key technologies	Beginner	Intermediate	Advanced
Data security • Endpoint and device security • Network microsegmentation • Two-factor authentication • Privilege identity management • Data encryption and loss prevention • Vulnerability risk management • Security analytics (NAV, UBA, SIM) • Patch management • Threat intelligence and hunting (external threat intel, TIP, EDR, MDR) • Security automation and orchestration	**Strategy:** Begin to implement Zero Trust, manage identities, encrypt data, and protect apps that access sensitive data. **Technology priorities:** • Architect and enforce segments of control around sensitive data and apps. • Use identity and access management to limit and strictly enforce access control. • Secure all resources and establish security operations fundamentals.	**Strategy:** Advance Zero Trust, identity management, and data security and add threat detection and response capabilities. **Technology priorities:** • Create more granular microperimeters of control around sensitive data and apps. • Implement two-factor authentication (2FA) and privilege identity management (PIM). • Deploy security analytics solutions to monitor network and user behavior. • Implement data loss prevention (DLP) across all extrusion points. • Develop capabilities to identify, prioritize, and remediate all critical vulnerabilities. • Automate repetitive low-risk tasks in the security operations center.	**Strategy:** Complete and extend Zero Trust, advance threat intelligence and threat hunting, and aggressively automate security operations. **Technology priorities:** • Consolidate, analyze, and adapt multiple threat intelligence sources. • Use threat hunting to reduce attacker dwell time. • Automate and orchestrate complex human and machine tasks.

FIGURE 1 Focus On Four Technology Areas To Drive Cybersecurity And Privacy (Cont.)

Key technologies	Beginner	Intermediate	Advanced
Cloud governance • Cloud security gateway/cloud access security broker • Cloud workload security • Single sign-on • Identity access management and governance • Security analytics • Customer relationship management platform • API gateway • Web application firewalls • DDoS • Runtime application self-protection • Secrets management • Incident response • Disaster recovery and business continuity	**Strategy:** Create and maintain compliance and reduce overall risk as the business embraces cloud as a preference. **Technology priorities:** • Discover sanctioned and unsanctioned cloud applications. • Encrypt sensitive cloud data in-flight and at-rest by default. • Work with IAM pros to provide single sign-on and provisioning integration. • Integrate log files and other telemetry from all cloud environments. • Protect your web applications against common attacks. • Continuously assess and provide proof of compliance.	**Strategy:** Develop a comprehensive cloud governance and security strategy as the business aggressively utilizes cloud deployment. **Technology priorities:** • Control access to cloud workloads based on user, device, role, and sensitivity. • Deploy tools that provide visibility, analytics, and detection for cloud workloads. • Deploy secrets management to avoid transferring sensitive data. • Add additional protections for fast-moving and legacy applications.	**Strategy:** Use governance and security capabilities to accelerate cloud adoption for speed, fluidity, and connection. **Technology priorities:** • Optimize protections for customer-facing and revenue-generating apps. • Simulate responses to cloud outages and incidents. • Rotate and generate secrets to enhance security. • Enforce secure communications with all APIs.

FIGURE 1 Focus On Four Technology Areas To Drive Cybersecurity And Privacy (Cont.)

Key technologies	Beginner	Intermediate	Advanced
Technical innovation • IoT platform • Prerelease application security scanning tools (SAST, DAST, IAST) • Software composition analysis • Mobile security suites • Runtime application self-protection (RASP) • Application hardening • Bot management • Signing	**Strategy:** Protect the brand from poor risk management and ethics failures. **Technology priorities:** • Establish AppDev security fundamentals to protect customers and retain their trust. • Manage critical open source components developers rely on to develop apps fast. • Add additional security to protect customers using virtual agents. • Build security into customer-facing IoT solutions. • Implement least privilege for RPA.	**Strategy:** Protect the brand from advanced threats and novel attacks of the data economy. **Technology priorities:** • Deploy brand protection and monitoring tools. • Automate application prerelease security testing. • Tamper proof mobile and IoT applications. • Guarantee the fidelity of web applications and workloads. • Operationalize open source consumption by application development.	**Strategy:** Build robust brand resilience by ensuring brand experience aligns with the brand promise for privacy, cybersecurity, and overall trust. **Technology priorities:** • Protect the integrity of the data your business makes decisions on. • Implement autopatching tools as part of prerelease application scanning. • Move prerelease testing as early as possible in the software delivery life cycle. • Optimize the use of open source components.

No. 1. Data Governance: Know Your Data To Reduce Essential Risks

Data is the lifeblood of today's digital businesses. Sophisticated cybercriminals want to steal it, employees and partners can abuse it, and regulators can use it to launch investigations and levy massive fines. For your business to thrive in the data economy, you'll need to build strong data governance capabilities. To do this:

› **Develop core capabilities to inventory, map, and classify sensitive data.** The first step in protecting data from cybercriminals and intentional and unintentional privacy abuses is to understand four things: 1) what you have; 2) how you handle and store it; 3) how you use it to serve customers and make decisions; and 4) how you share and monetize it. Once you know the answers, you can adjust policies and deploy the right controls. Here, you can opt for specialized solutions for data discovery, classification, and flow mapping, for consolidated solutions like IBM Guardium and Heureka Software, or for features in other solutions like TITUS and Nuix.

- **Adopt solutions to continuously track personal data.** Personally identifiable data about your customers or employees belongs to them, not to your firm, and they can ask you to show it, amend it, or delete it.[2] Data management platforms that index or catalog the data (vendors like Global IDs and Datum); data discovery, classification, and flow-mapping tools; and even solutions that scan your network (like Symantec and DigitalGuardian), can all help you keep track of the data.
- **Encrypt sensitive data by default.** Once you've identified your most sensitive data, the best way to protect it is to obfuscate it. Obfuscating data through encryption, tokenization, and other methods renders the data useless to cybercriminals who want to sell it on the underground market. If they can't use or sell it, they won't steal it. Encryption can also protect against privacy abuses, even when your firm transfers or shares data. And encryption that follows regulators' guidelines also helps mitigate the risk of fines and enforcement actions.
- **Use software to assess compliance posture and operationalize workflows.** You can no longer rely on spreadsheets to track your privacy programs, because regulators require you to provide evidence of your compliance efforts on a continuous basis and without notice. Maturing privacy teams need a technology solution like OneTrust or SAI Global to adequately scale, manage, and report on privacy program processes as well as to initiate auditable workflows.
- **Implement archiving and eDiscovery solutions.** Archiving tools are indispensable for any firm in a regulated or litigious industry.[3] Although you may not buy them specifically for cybersecurity or privacy, archiving tools can help improve security, and Forrester includes them as part of our data security and control framework. It's much easier to focus your cybersecurity efforts on protecting the firm's most critical information assets as opposed to all of your digital debris. eDiscovery technologies provide capabilities to streamline and operationalize defensible discovery processes in response to events such as litigation, internal investigations and audits, freedom of information requests, and regulatory action.[4]

No. 2. Data Security: Move To A Data-First Zero Trust Strategy

Data-sharing agreements, partnerships, and connectivity are all core components of digital supply chains, which are as important as physical supply chains. In the data economy, security strategies must center on data. You will need to adopt Forrester's Zero Trust model for moving to a data- and identity-centric cybersecurity strategy. To do this:

- **Architect and enforce segments of control around sensitive data and apps.** If you isolate your sensitive systems and data into a series of network segments, then a breach of the network won't give cybercriminals or malicious insiders free rein across the entire environment. You'll want to design your network segments to reflect the flow of transactions across the ecosystem and how users and other systems access sensitive data. You can enforce the segments with hardware or software that can granularly control network access, like firewalls from Cisco and Palo Alto Networks or software solutions from VMware and Illumio.

- **Use identity and access management to limit and strictly enforce access control.** Identity and access management (IAM) technology allows your firm to: 1) manage customer identities, preferences, and profiles across channels; 2) let customers control how you use their data, as required by the EU GDPR; 3) provide secure, least-privilege access to sensitive data for employees and partners; 4) secure access to all the interfaces that customers choose; and 5) use their data to identify (and banish) malicious actors.[5]
- **Secure all resources and establish security operations fundamentals.** Under Zero Trust, all resources must be accessed securely, regardless of location or hosting model. Assume that all traffic is threat traffic until you've authorized, inspected, and secured it. Another critical capability is vulnerability risk management; if you don't have a process to identify, prioritize, and remediate critical vulnerabilities in your environment, you are failing key security responsibilities.[6]

No. 3. Cloud Governance: Help The Business Embrace Cloud While Reducing Risk

Whatever stage you're at in your cloud journey, if you're at the beginner level for cybersecurity and privacy, your principal task here is to reduce overall risk and maintain compliance. To do this:

- **Discover sanctioned and unsanctioned cloud applications.** Use an automated method to discover cloud applications in use (e.g., personal Box or Dropbox accounts, unprotected customer applications) and understand the data traffic to these applications.[7] But don't immediately disallow these services. Instead, work with business leaders to provide oversight and security controls. Third-party cloud security gateway solutions such as those from Symantec and McAfee (Skyhigh Networks) provide capabilities such as cloud app discovery and monitoring, user activity monitoring, data loss prevention, and encryption.[8]
- **Encrypt sensitive cloud data in-flight and at-rest by default.** Just as with your on-premises apps and workloads, you must encrypt data in-flight and at-rest in the cloud. Preferably, you should work with a third-party cloud security vendor (cloud security gateway vendors like CipherCloud or data security specialists like MicroFocus Voltage) that allows you to store encryption keys either on-premises or in their cloud offering.[9] This greatly reduces the likelihood of a data breach and gives you full control of encrypted sensitive information in the cloud — even if a court forces the cloud provider to surrender all its data.
- **Work with IAM pros to provide single sign-on (SSO) and provisioning integration.** Limiting and strictly enforcing access control is a core pillar of Zero Trust, and this extends to cloud workloads. In addition, as cloud workloads proliferate, you can only ensure a seamless user access experience to these workloads if you provide SSO for users and integrated provisioning for administrators. SSO requires sharing user information between on-premises and cloud-based directories and workloads, while provisioning requires that identity management systems have connectors to IaaS platforms and SaaS applications.

- **Integrate log files and other telemetry from all cloud environments.** An Australian manufacturer suffered a data breach and wanted to use a major customer relationship management (CRM) platform's access log files to investigate the incident. It turns out their access to the logs was limited. Your IaaS or SaaS provider may not provide you access to forensic and log information because it may contain information about other tenants. You'll also need an SLA from your cloud provider about speed and method of access to those log files.
- **Protect your web applications against common attacks.** To achieve PCI DSS compliance, you must have a web application firewall (WAF) or similar tool protecting your application.[10] WAFs from vendors like Akamai Technologies and F5 Networks will not only protect against application attacks but they also provide a layer of defense for any weaknesses or vulnerabilities in your apps. Cloud providers now offer their own WAFs, but often these are limited in security protection. Place WAFs in front of all web applications and APIs.
- **Continuously assess and provide proof of compliance.** Compliance and audit stakeholders need assurances that the firm meets regulatory mandates. This includes periodic reports on cloud security such as data loss prevention effectiveness, ad hoc and customizable reports, and compensating controls that cloud security solutions provide in the form of canned policy templates for regulations like PCI. Tech leaders also need to be proactive about data residency. Privacy laws such as the EU's GDPR limit the transfer of its citizens' PII outside of EU member countries. Cloud providers increasingly support data residency, but encryption can give tech leaders more control in satisfying data residency requirements.

No. 4. Technology Innovation: Protect The Brand From Missteps

Technologies like automation, individualization, virtual assistants, edge computing, external API services, IoT, and digital process automation will help businesses improve agility, customer experience, and revenue growth.[11] But they also increase your attack surface. CIOs, CISOs, and other tech leaders must balance innovation with risk management discipline. To do this:

- **Establish AppDev security fundamentals to protect customers and retain their trust.** Your websites and mobile apps are mosaics of home-brewed and third-party code riddled with weaknesses like SQL injection and cross-site scripting. To deny attackers those easy wins, implement automated application security testing solutions. Use tools from vendors like CA Veracode and Synopsys to do static application security testing (SAST) to fully test all conditional code and dynamic application security testing (DAST) tools from vendors like Qualys and Rapid7 to fully test dynamically generated code.[12]
- **Manage critical open source components developers rely on to develop apps fast.** Developers of websites, mobile apps, and IoT apps are all using open source components to innovate faster. These components provide common functionality and allow developers to focus on differentiating

features. However, they also represent your biggest risk.[13] Scan all applications using software composition analysis (SCA) tools from vendors like Synopsys and WhiteSource to create a list of what open source components exist in your code and to remove or upgrade vulnerable components.[14]

- **Add additional security to protect customers using virtual agents.** Today, virtual agents such as Alexa, Google, or Siri have extremely limited authentication; some unwisely allow users to authenticate with static four-digit codes.[15] The only method to improve authentication is to rely on two-factor authentication (2FA) that uses alternate devices such as mobile phones. Explore what services your company is exposing using virtual agents and determine if 2FA is needed.
- **Build security into customer-facing IoT solutions.** IoT solutions have limited storage capacity and, as a result, transfer data to a more permanent data store. This data then passes through different wireless carriers, making it especially vulnerable to attacks. Implement encryption for your data in-flight and any at-rest data that must temporarily reside on the IoT device. For any IoT platform your developers are using, determine upfront what the platform is doing with the data to extract insight, value, and revenue from data stored in it.[16]
- **Implement least privilege for RPA.** Forrester estimates that there will be more than 4 million robots doing office and administrative work as well as sales and related tasks by 2021.[17] However, when anyone can create, modify, or deploy these robots using robotic process automation (RPA) tools, employees across legal, human resources, development, operations, and finance could all be making contributions. Create clear roles for employees who can create, modify, and deploy robotic processes to adhere to segregation of duties rules. Enforce these roles using IAM tools.

Endnotes

[1] Forrester provides CIOs with a self-assessment tool that evaluates your current cybsersecurity and privacy program and guides you to your next-best actions. Look for Forrester's upcoming report "Assessment: Gauge Your Cybersecurity And Privacy Maturity."

[2] Both GDPR and the new California Consumer Privacy Act 2018 demand that organizations satisfy these customers' requests quickly, and certainly your customers expect that you do so, too. You need to know where data is, where it came from, who owns it, and with whom you shared it.

[3] Regulated industries have rigorous requirements for eDiscovery, regulatory compliance, and execution of corporate retention policies. Recreating a digital experience to meet a legal requirement is a difficult task when personalized and contextualized content results in a different web experience for different types of website visitors. The ability to stay ahead of the curve here determines success of web modernization efforts and personalized customer experiences. See the Forrester report "How To Archive Personalized, Contextualized Web Experiences."

[4] Security and risk (S&R) professionals should understand the value they can expect from an eDiscovery technology provider and select vendors based on size and functionality. For more information, see the Forrester report "Now Tech: eDiscovery Technologies, Q3 2018."

[5] See the Forrester report "The Future Of Identity And Access Management," see the Forrester report "The Forrester Tech Tide™: Identity And Access Management, Q4 2017," and see the Forrester report "The Five Milestones To GDPR Success."

Forrester outlines the technologies that technology leaders should prioritize to kick-start customer engagement and lay the groundwork for continued growth including: web and mobile interfaces for customer engagement; data and analytics to understand customers; identity management to protect and serve customers; and cloud computing to move to the future of software. See the Forrester report "Reset Your Technology Foundation For Customer Engagement."

EU GDPR: European Union General Data Protection Regulation.

[6] The second most common method of external attack is the exploitation of software vulnerability. For more information about vulnerability risk management tools, see the Forrester report "The Forrester Wave™: Vulnerability Risk Management, Q1 2018."

[7] If you don't know where your sensitive data is going, you can't protect against data breaches.

[8] For more information about cloud security gateway solutions, see the Forrester report "The Forrester Wave™: Cloud Security Gateways, Q4 2016."

[9] For more information about cloud security gateway solutions, see the Forrester report "The Forrester Wave™: Cloud Security Gateways, Q4 2016."

[10] For more information about WAFs, see the Forrester report "The Forrester Wave™: Web Application Firewalls, Q2 2018."

[11] Forrester has identified 12 emerging technologies with massive disruptive potential; their impact will be seen across a range of products, services, and solutions. This report helps CIOs zero in on the technologies most worthy of their focus, strategic planning, and investment. See the Forrester report "The Top Emerging Technologies To Watch 2018."

[12] For more information about SAST and DAST tools, see the Forrester report "Vendor Landscape: Application Security Testing" and see the Forrester report "The Forrester Wave™: Static Application Security Testing, Q4 2017."

[13] For more information about how open source vulnerabilities represent your biggest risk, see the Forrester report "Top Cybersecurity Threats In 2018."

[14] For more information about SCA tools, see the Forrester report "Vendor Landscape: Software Composition Analysis" and see the Forrester report "The Forrester Wave™: Software Composition Analysis, Q1 2017."

[15] For more information on how to secure virtual agents of today and the intelligent agents they will become using IAM tools, see the Forrester report "IAM For Intelligent Agents."

[16] For more information about IoT platforms, see the Forrester report "IoT Delivery Best Practice: Adopt A Domain-Specific Platform."

[17] For more information about RPA, see the Forrester report "The Forrester Wave™: Robotic Process Automation, Q2 2018."

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.