Assess Your Cybersecurity And Privacy Maturity

Assessment: The Cybersecurity And Privacy Playbook

by Enza Iannopollo and Renee Murphy
September 25, 2018

Why Read This Report

Weak cybersecurity and privacy practices reflect poorly on your company's brand, making it less attractive to customers, partners, employees, and investors. CIOs who want to drive business success must regularly assess their organization's approach to cybersecurity and privacy, then partner with their security and privacy colleagues to improve their programs. This report details the key capabilities that CIOs should focus on when measuring the maturity of their cybersecurity and privacy programs, providing a framework and tool for self-assessment.

Key Takeaways

Mature Cybersecurity And Privacy Capabilities Are Key To Succeed In Digital Business

As digital disruption changes the competitive landscape in every major industry, the way companies collect, process, and act upon data will dictate their success. Without mature security and privacy capabilities, companies will be hamstrung by complicated regulatory requirements and constant external attacks.

Improved Maturity Hinges On Documentation And Metrics

Data intelligence allows firms to take the next best decision to achieve a goal or advance their strategy. Building cybersecurity and privacy maturity requires the same approach: Documentation and metrics fuel organizations' knowledge about their oversight, processes, technologies, and people. This intelligence triggers actions that fuel efficiency and competitive advantage.

Assess Your Cybersecurity And Privacy Maturity

Assessment: The Cybersecurity And Privacy Playbook

by Enza Iannopollo and Renee Murphy
with Christopher McClean, Stephanie Balaouras, Elsa Pikulik, and Peggy Dostie

September 25, 2018

Cybersecurity And Privacy Are Foundations Of Healthy Digital Business

Wired Magazine's March 2018 cover showed Facebook CEO Mark Zuckerberg' face as it would appear after a boxing match, suggesting the reputational damage from perceived lack of vision, poor business decisions, and dicey choices regarding external partners and user data.[1] Shortly after that, the Cambridge Analytica story broke, and in July, Facebook announced such poor financial performance that it lost $120 billion in value.[2]

Like Facebook, today's most successful businesses are those that have found ways to effectively collect, process, and use massive amounts of data.[3] However, as Facebook's beating shows, companies that rely on their prowess with data to drive revenue and customer growth without implementing appropriate controls can soon see their customers, users, employees, and investors lose faith and their brand value tumble. Digital business success requires strong cybersecurity and privacy programs.

Firms That Understand Cybersecurity And Privacy Excel At Four Competencies

Measuring and improving your firm's cybersecurity and privacy programs to support digital business can seem an overwhelming task; however, there are key capabilities that any company can implement. These key capabilities fall under the four competencies of oversight, process, technology, and people and culture (see Figure 1).

- **Oversight.** Capabilities in this competency align security and privacy with business objectives. This competency includes capabilities for developing strategy, adhering to internal and external requirements, managing risk, and effectively governing decisions and resources. These capabilities are the foundation that allows the CIO to align and guide all other relevant capabilities. They help the CIO make sure that cybersecurity and privacy efforts support and drive business objectives, rather than get in their way.
- **Process.** Capabilities in this competency embed security and privacy into business operations. This competency describes how well the organization implements security and privacy into its customer-facing products and services as well as its own internal processes. It also covers the

FORRESTER®

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

extension of security and privacy requirements to third-party partners and the ability to respond quickly to external questions from stakeholders such as customers, auditors, and regulators. With these capabilities, the CIO raises the level of confidence throughout the organization and among stakeholders that data controls are well established and operating effectively.

› **Technology.** Capabilities in this competency control the collection, storage, and use of data. This competency includes capabilities for data governance, data security, cloud governance, and technical innovation. It helps CIOs and their organizations set and enforce policy to protect their most valuable asset: data. The elements in this competency help firms protect the confidentiality of sensitive information without inhibiting its use for legitimate business purposes.

› **People.** Capabilities in this competency build a corporate culture that cares about security and privacy. This competency describes how well the organization communicates cybersecurity and privacy efforts, aligns these efforts across the organization, embeds a companywide cybersecurity and privacy culture, and manages relevant skills. It helps CIOs meet cybersecurity and privacy objectives by effectively allocating responsibilities throughout their organization, the broader business, and the extended ecosystem.

FIGURE 1 Cybersecurity- And Privacy-Savvy Businesses Excel At Four Competencies

Sixteen key capabilities across four competencies enable customer obsession.

Oversight: strategy, adherence, risk management, governance
1) Do you consider aspects of cybersecurity and privacy when developing your technology strategy?
2) Do you have the capability to catalog requirements from third parties (including customers, regulators, etc.) and apply those requirements to IT efforts and investments?
3) Do you have the capability to articulate and address risks related to privacy, cybersecurity, data integrity, brand protection, and ethical behavior?
4) Do you have the capability to set decision structures, roles, and responsibilities across your organization to meet established security and privacy goals?
Process: product security and privacy; internal security and privacy; third-party risk management; response to customers, auditors, and regulators
5) Do you support the business' efforts to bring products and/or services to market in a way that dynamically identifies and mitigates security and privacy risks?
6) Do you manage security and privacy risks related to your organization's internal operations?
7) Do you manage security and privacy risks in your partner ecosystem?
8) Do you promote transparency and openness about your organization's security and privacy efforts with external stakeholders?
Technology: data governance, data security, cloud governance, technical innovation
9) Do you have the capability to collect, classify, manage, and delete data based on business needs, privacy requirements, and cybersecurity risk tolerance?
10) Do you have the capability to protect important, sensitive, and private data, whether it's stored on-premises, with a third party, or in the cloud?
11) Do you have the capability to monitor and enforce controls to protect data and assets in cloud environments?
12) Do you have the capability to help drive technical innovation in your organization in order to stay ahead of market trends and customer expectations while protecting against unexpected threats and privacy issues?

FIGURE 1 Cybersecurity- And Privacy-Savvy Businesses Excel At Four Competencies (Cont.)

People and culture: proactive, external communication; organizational alignment; cybersecurity and privacy culture; skills management
13) Do you have the capability to promote your organization's security and privacy practices to customers and other external stakeholders?
14) Do you have the capability to establish privacy and security responsibilities among internal stakeholders throughout the organization?
15) Do you have the capability to guide employee behavior toward responsible security and privacy practices?
16) Do you have the capability to define and achieve sufficient staff resources and expertise to support security and privacy objectives?

Assess Your Cybersecurity And Privacy Maturity

The 16 capabilities that make up each of the four competencies are crucial for insights-driven businesses to succeed. To evaluate the maturity of your organization's approach to cybersecurity and privacy, take stock of the behaviors it exhibits for each capability. The results will give you specific components to improve upon to raise each capability's maturity level (see Figure 2):

- **Repeatable capabilities exhibit consistent actions and decisions.** Capabilities at this level are usually built on institutional knowledge, which are passed along as informal requirements to various business capabilities. Often, teams responsible for these capabilities have an established set of assumptions about how each team member contributes to its success; however, it's likely difficult to assess their effectiveness because objectives aren't clearly articulated.
- **Defined capabilities operate according to documented policy and responsibilities.** Written policies, procedures, roles, and responsibilities are attributes of "defined" capabilities. They are predictable and understood, and it's typically clear whether responsible parties are executing their assigned duties. A capability usually gets to this level because of a regulatory requirement or because a decision maker determines that it's important for the company's success.
- **Measured capabilities generate data to track performance.** Monitoring the performance of security and privacy capabilities is the key indication that it's reached a "measured" level of maturity. This generally means that there are more than simply defined processes and responsibilities; there are desired outcomes against which the organization can measure performance. There are also consumers of the generated data, who typically have a stake in the capability's success.

› **Optimized capabilities continually improve in support of business success.** Capabilities at this level are strongly integrated and aligned to the business. Responsible parties use available metrics to judge their performance and make adjustments to achieve a balance of business performance and risk management objectives. Optimized capabilities often are those that have embraced automation in their assessments and remediation actions.

FIGURE 2 Four Indicators Help Determine Maturity Level

Four indicators help determine maturity; multiple may apply
Repeatable: We follow a process to do this.
Defined: We have a published policy in place for this.
Measured: We have metrics in place for this.
Optimized: We regularly review the metrics we use for this.

Your Capabilities Score Determines Your Firm's Overall Maturity Level

Assessing each capability helps you identify whether your organization's cybersecurity and privacy efforts are at the beginner, intermediate, or advanced level. You can apply these maturity levels to your oversight, process, technology, and people competencies to determine how best to allocate resources for improvement:

› **Beginner level: Build the foundation for cybersecurity and privacy mastery.** Firms at this level of maturity are executing only basic cybersecurity and privacy efforts, with most capabilities being either nonexistent or ad hoc. To improve, they must raise the level of institutional knowledge to create consistency, then move to document policies, procedures, and responsibilities. They may even publish a basic framework of risks and controls to help asset owners, product managers, and other stakeholders more formally identify and manage risks.

› **Intermediate level: Measure the effectiveness of your programs continuously.** Firms at this level of maturity have repeatable and defined efforts to strengthen cybersecurity and privacy, but they generally lack a quantifiable understanding of their performance. To improve, they should introduce metrics that help identify areas of excellence, weaknesses, and threats that require immediate attention. A big step in this process is to determine the desired business and risk management outcomes, so metrics more clearly guide decision makers toward improvement.

› **Advanced level: Optimize your programs to build competitive advantage.** Firms at this level of maturity have a portfolio of cybersecurity and privacy metrics, and they're ready to act in support of continued improvement. These firms have a robust cybersecurity and privacy culture and a solid governance structure to deal with changes to regulations, threats, business needs, and customer expectations. They are all about promoting excellence inside and outside their organizations, which also means driving third-party partners to continually improve. At this stage, firms should be constantly looking for ways to connect their security and privacy efforts directly to business performance metrics like customer satisfaction and loyalty.

Supplemental Material

Online Resource

The online version of this report includes a maturity assessment. Click the link at the beginning of this report on Forrester.com to access the assessment.

Endnotes

[1] Source: "What Happened To Zuckerberg? Here's How Our March 2018 Cover Was Created," Wired, February 12, 2018 (https://www.wired.com/story/facebook-about-the-cover/).

[2] Source: Emily Stewart, "The $120-billion reason we can't expect Facebook to police itself," Vox, July 28, 2018 (https://www.vox.com/business-and-finance/2018/7/28/17625218/facebook-stock-price-twitter-earnings).

[3] Becoming insights driven is now the holy grail of business transformation, and many firms are making concrete progress toward this end. However, change doesn't come easy. In this report, chief data officers (CDOs), chief analytics officers (CAOs), and other insights leaders offer CIOs best practices in preparing their organizations for change, executing on the new insights-driven strategy, and nurturing the new insights-driven culture. See the Forrester report "Data Leaders Weave An Insights-Driven Corporate Fabric."

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.