Build The Business Case For Cybersecurity And Privacy

Business Case: The Cybersecurity And Privacy Playbook

by Sean Ryan

August 14, 2020

Why Read This Report

Mega data breaches will often spur organizations to invest in cyber security. However, if the approach is reactive and unplanned, then it's a wasted opportunity. Use this report to structure a sound business case for cybersecurity and privacy investments that provides assurance to the stakeholders and value to the business.

This is an update to a previously published report.

Key Takeaways

Map The Security Plan To Business Outcomes
Structure a business plan for clearly defined benefits and expected outcomes by aligning the plan to four levels of value: 1) better efficiency; 2) risk mitigation; 3) increased revenue; and 4) improved company performance.

Use Innovative Security Practices To Delight Customers And Differentiate Offerings
As business customers and consumers expect more from the companies they associate with, strong security and privacy capabilities can lead to customer preference over competitors and customer loyalty. The best programs may even warrant premium prices or generate revenue on their own.

FOR CIOS

Build The Business Case For Cybersecurity And Privacy

Business Case: The Cybersecurity And Privacy Playbook

by Sean Ryan
with Merritt Maxim, Andras Cser, Madeline Cyr, Stephanie Balaouras, Elsa Pikulik,
Benjamin Corey, and Peggy Dostie

August 14, 2020

Table Of Contents

Recommendations

Related Research Documents

Assess Your Cybersecurity And Privacy Maturity

Benchmark Your Cybersecurity And Privacy Maturity, 2020

Security Budgets 2020: New Threats Bring New Priorities

FORRESTER®

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

Provide Cybersecurity And Privacy Assurance For All Stakeholders

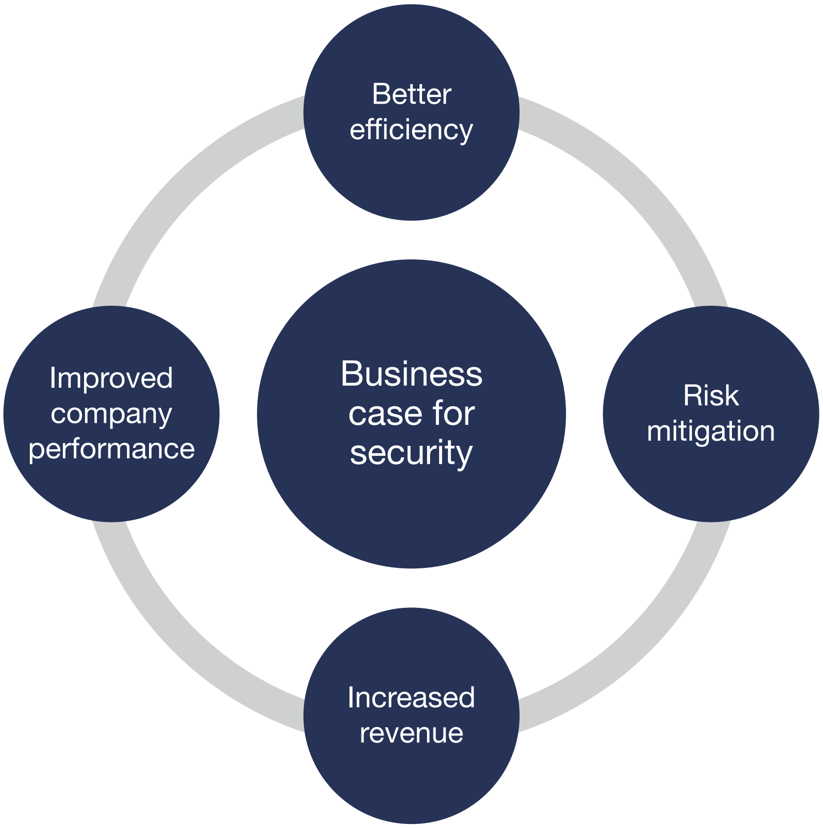
Boards of directors and executive leadership teams are increasingly cognizant of the dangers of mega breaches, where costs can run from $40 million to $350 million.[1] They're aware of the brand reputation damage from betraying customer trust, such as recent events that led to a $5 billion fine for Facebook.[2] On top pf this, the COVID-19 pandemic is causing unprecedented business disruption. Executives must acknowledge these challenges in the business case, but leading with fear is not a winning approach. S&R pros must emphasize how the security plan will mitigate cyber risks, improve operational efficiency, and aid in revenue growth. As S&R pros build their cybersecurity and privacy business plan, they should keep the following factors in mind:

- **Economic uncertainty means you need a laser focus on key security priorities.** The current COVID-19 pandemic-induced economic turmoil is forcing organizations to make tough budget-cutting decisions.[3] This requires you to identify the most mission-critical security and privacy controls to avoid unintended consequences if more severe cuts are required.
- **Any adjustments in investments will require clear and measurables outcomes.** The most common security metrics either use simple-to-gather data without much meaning or basic compliance checks that are difficult to distinguish from audits.[4] Going forward, ensure that metrics connect to quantifiable business objectives such as revenue, margin, growth, or customer satisfaction. In today's competitive business climate, any cost increase with no commensurate benefit will be squashed.
- **Business continuity is now tied to secure access for remote workforces.** If the infrastructure that validates employee and partner credentials and access to critical systems goes down without a backup system, business operations will grind to a halt. A banking firm told us that its multifactor authentication (MFA) for remote workers had gone down for a full day prior to the pandemic. Once the entire workforce had to go remote, it became imperative for the organization to build resiliency into its multifactor authentication infrastructure.[5]
- **Customers are paying attention to the privacy of their personal data.** Violating GDPR, CCPA, or other customer privacy laws brings fines, but loss of customer trust will mean loss of customer lifetime value. Customers are becoming more privacy savvy, with 73% of US online adults voicing concern that their data could be permanently recorded and accessible to anyone without their knowledge.[6]

Align Your Cybersecurity Business Case To Four Levels Of Value

A compelling cybersecurity and privacy business case should align to four goals: 1) better efficiency; 2) risk mitigation; 3) increased revenue; and 4) improved company performance (see Figure 1). Structuring a business plan along these lines provides clear value and identifies the expected business value. Further, you will be better able to prioritize investments in the face of difficult tradeoffs stemming from potential budget constraints.

FIGURE 1 The Four Levels Of Value From Cybersecurity And Privacy Investments



Improve Security And Privacy Efficiency With Targeted Investments

Your firm's internal processes and tools are the bedrock of its productivity and ability to compete effectively. Many aspects of information and technology management have important cybersecurity and privacy implications, including controlling access, updating systems, and managing change. Without investment, however, these efforts are often manual. Justifying budget for cybersecurity and privacy technologies may be as simple as showing more work done in less time:

› **Speeding up processes reduces costs.** For many aspects of cybersecurity and privacy, new investments might simply reduce the time staff needs to accomplish the task at hand. A large North American manufacturing company moved from an on-premises access management solution to an Azure AD identity-as-a-service (IDaaS) solution and was able to automate password resets, optimize password policies, and capture metrics for improved decision making that in the past was done in a manual and ad hoc manner. This reduced the number of password resets by 1,000 per month, thus greatly reducing help desk costs. Furthermore, automating user group capabilities reduced troubleshooting from hundreds of hours per year to five days to resolve.

- **Automating capabilities can both embed and enhance cybersecurity and privacy.** Boosting efficiency can also extend the reach of cybersecurity and privacy capabilities within the business. A North American telco standardized on a single container platform, creating a unified DevSecOps team responsible for imbuing security at build time into newly built machine instance images. By creating a standard that applied to a much larger percentage of new development, the team helped developers produce 30% more applications with security baked in, in the same amount of time.

Reduce Security And Privacy Risks For Employees And Customers

A key objective for cybersecurity and privacy investments is to reduce the cost of accidents, incidents, breaches, and violations. A recent trend in the industry has seen CISOs and CIOs try to quantify the expected annual financial loss of every major category of risk, but there's a much more practical way to quantify risk: CIOs can evaluate likelihood based on such factors as the existence of known attack techniques and susceptibility of a target to an attack, and they can evaluate impact using such factors as scope of the loss and expected recovery time. For every category of risk, assessments should consider four possible types of impact:

- **Outages and reallocation of resources.** Tools and technologies that prevent attacks help companies maintain high availability of key systems and processes, and they reduce the likelihood that staff will have to stop their primary work to respond to issues and incidents. Forrester's interviewees expect corporate data breach victims to now have improved security measures in place that will make them less likely targets for hacking. Preventing new attacks or having strong contingencies in place to reduce the impact of successful attacks will minimize disruptions to the company's operations.[7]

- **Loss of customer trust and loyalty.** In today's environment of ubiquitous data breaches, clients' expectations about your company's security are constantly increasing. In certain industries and geographies, clients even consider security a competitive differentiator.[8] In such cases, an investment in cybersecurity and privacy that reduces the risk of data theft or privacy abuse helps avoid security incidents that might cause customers to defect to a competitor they perceive as being more secure.

- **Fines, lawsuits, settlements, and other legal costs.** GDPR entered into force in May 2018 and has been followed by others such as CCPA, which is set to take effect by October 2020.[9] As lawmakers continue to look to make examples out of companies that have suffered a data breach, protecting your clients' data can save you from regulatory fines and sanctions.

- **Direct financial losses.** While attacks that interrupt operations, tarnish the brand, or invoke a regulatory settlement all eventually hurt a company's finances, some attacks have a more direct effect on the balance sheet. Investments in antifraud technologies, however, can directly reduce the number of illegitimate transactions that a company has to cover, and improvements to that technology can also reduce the number of false positives that block or delay financial transactions.[10]

Mature Programs Tie Cybersecurity Performance To Increased Revenue

Although assessing the value of security and privacy investments in terms of risk reduction can be a crucial exercise, it might keep CIOs in the same rut of trying to measure the value of nothing happening. A more successful approach to building a business case will consider revenue and growth as well: With better security, and a more secure customer journey, clients are more likely to be willing to start and maintain a business relationship with you.[11] To build a comprehensive view of value, you need to think about value protection as well as value creation:

- **Security and privacy give customers a reason to prefer your firm over others.** If your organization demonstrates thought leadership and investment in security and privacy, it will increase the willingness of clients to do business with you.[12] This trend is abundantly clear in B2B firms that must fill out a constant stream of lengthy security questionnaires before they're considered a viable option. In B2C firms, the examples are more diverse but no less clear. After implementing a more secure electronic signature process, a US credit union saw a 97% lift in online lending, suggesting that when given an option, customers sought security and convenience.

- **Advanced security options may warrant premium pricing.** More-advanced internal cybersecurity and privacy capabilities will allow you to improve the security in your products as well. Your engineering team will be able to build enhanced sensors, telemetry, monitoring, and alerting into your solution to improve its security. While no customer wants to pay extra for security fundamentals, they may be willing to pay for more-advanced security and privacy features, as is the case when customers of the largest public cloud providers decide to add security capabilities on top of their broader cloud engagements.

- **Truly differentiated capabilities may make good standalone offerings.** As you build out your cybersecurity and privacy capabilities, your organization's competency may be so strong that you can market your expertise and services to help other, less mature companies. After mastering compliance audits, a North American heavy equipment manufacturer started marketing its security consulting capabilities to third parties. Similarly, Axciom turned its internal know-your-customer identification service into an external product, and a European retailer used fraud management transactional and site navigational information to reposition its product portfolio.

Optimized Security And Privacy Programs Improve Overall Company Performance

Beyond the more tangible benefits around efficiency, risk reduction, and revenue growth, mature cybersecurity and privacy programs will have positive effects on company performance that will be harder to measure in the short term. That said, given how directly these additional benefits relate to the organization's competitive advantages and financial success, it's still important to consider that:

- **Better risk and compliance information increases agility.** Understanding the risk and compliance implications of business decisions can help a company serve new customers, adopt new technologies, or penetrate new markets faster than companies that don't. Companies that have invested in tools and processes to meet difficult GDPR requirements will find themselves in a great position to do business in other countries around the world adopting similar laws.[13] The same goes for working with new customers. References for the Forrester Wave™ of risk-based authentication said that these tools help them fast-track registration for customers who exhibited good behavior on other eCommerce websites, and allowed them to offer services and products in risky geographies (South America, Eastern Europe, Southeast Asia, etc.) where they have not been able to before.[14]

- **Stakeholders are drawn to brands with a strong security and privacy reputation.** Even more difficult to measure is the benefit of increased loyalty among customers, employees, and other stakeholders as a result of good cybersecurity and privacy. This benefit requires more than just strong capabilities; it requires a consistent pattern of doing the right thing. As a result of improved security and better self-service, clients mentioned that implementing services for customer identity and access management (CIAM) resulted in greater efficiency in customer acquisition, lower customer and shopping cart abandonment, and better conversion rates (customers signing up and buying on the site). Similarly, Experian found that 74% of consumers chose security as the most important element when buying online in 2019.[15] Over time, these improved customer experiences will clearly link to increased customer loyalty, satisfaction, and revenue.

Recommendations

Map Cybersecurity And Privacy Plan To Business Outcomes

Align privacy and security measures to the four levels business value in a way that maps your current and planned spending across these initiatives. This serves to provide clear direction on how to prioritize spending initiatives along with the any expected future spending changes. As you go through your cybersecurity strategic planning, incorporate the following considerations into your thinking:

- **Present efficiency gaining measures that don't sacrifice a secure posture.** Identify areas where lower-cost alternatives don't exist or would pose unacceptable risk, and protect these from budget cuts; for instance, secure privileged access to your most critical systems and databases. Once those are protected, look for areas to consolidate overlapping technologies and automate manual processes that can reduce costs and staffing requirements.

- **Involve business partners in driving value through improved security and privacy.** Many business operations today rely on the sharing of information and access to systems of external partners and suppliers. Bring these partners to the table as you look for ways to gain efficiencies, reduce risk, or drive new revenue opportunities.

- **Include evaluations of emerging technologies in your business case.** Belt-tightening measures naturally lead CIOs and CISOs toward a more conservative approach of looking to large, established security providers to consolidate vendors and drive costs down. However, continue to watch for emerging vendors that will help you innovate. Charge your security teams with identifying emerging vendors that offer strong potential to advance your cause along the four levels of value.
- **Seek out revenue-generating opportunities for security features.** As new technology projects are increasingly customer-facing, your old business case focusing on compliance levels and coverage just won't cut it. Look at your product roadmap to determine whether security and privacy capabilities might convince customers to choose your product over that of competitors, and either pay a premium for it or license it outright as a standalone product.

Endnotes

[1] Source: Dean Takahashi, "IBM security study: Mega data breaches cost $40 million to $350 million," VentureBeat, July 10, 2018 (https://venturebeat.com/2018/07/10/ibm-security-study-mega-data-breaches-cost-40-million-to-350-million/).

[2] Source: Rob Davies and Dominic Rushe, "Facebook to pay $5bn fine as regulator settles Cambridge Analytica complaint," The Guardian, July 24, 2019 (https://www.theguardian.com/technology/2019/jul/24/facebook-to-pay-5bn-fine-as-regulator-files-cambridge-analytica-complaint).

[3] On April 14, 2020, the International Monetary Fund projected that real GDP would fall in 2020 by 5% to 8% in the US, Canada, Japan, France, Germany, the UK, and most industrial markets, with China's and India's economies coming to a standstill. Source: "World Economic Outlook Reports," International Monetary Fund (https://www.imf.org/en/Publications/WEO).

[4] Difficulty creating meaningful metrics persists for chief information security officers (CISOs) despite a decade of discussion. Without good metrics, the security organization can't participate in business conversations alongside sales, marketing, finance, and operations. This report is a complete guide to metrics that CISOs can use to steer the security team's efforts, allocate resources strategically, and communicate results with stakeholders throughout the organization. We put aside platitudes like "talk to the business" in favor of detailed discussion points and practical examples. See the Forrester report "Remove The Mystery From Security Metrics."

[5] Source: Sean Ryan, "A Spike In Home Workers Raises MFA Resilience Questions," Forrester Blogs, March 17, 2020 (https://go.forrester.com/blogs/a-spike-in-home-workers-raises-mfa-resilience-questions/).

[6] Source: Forrester Analytics Consumer Technographics® Global Online Benchmark Survey (Part 2), 2019.

[7] Cybercriminals are using more-sophisticated attacks to steal valuable intellectual property and the personal data of your customers, partners, and employees. Their motivations run the gamut from financial to retaliatory. With enough time and money, they can breach the security defenses of even the largest enterprises. You can't stop every cyberattack. However, your customers expect you to respond quickly and appropriately. If you contain a breach poorly and botch the response, you will pay millions in remediation costs and lost business, and it will ruin your firm's reputation. See the Forrester report "Planning For Failure: How To Survive A Breach."

[8] Source: Will Foret, "Using Cyber Security As A Competitive Advantage," Forbes, October 9, 2019 (https://www.forbes.com/sites/forbesbusinesscouncil/2019/10/09/using-cyber-security-as-a-competitive-advantage/#1bac59227ff7).

[9] Source: David M. Strauss and Malia Rogers, "Business Considerations for Complying With the Final CCPA Regulation," Law.com, June 19, 2020 (https://www.law.com/corpcounsel/2020/06/19/business-considerations-for-complying-with-the-final-ccpa-regulation/).

[10] See the Forrester report "The Forrester Wave™: Anti-Money Laundering Solutions, Q3 2019."

[11] Source: Alla Valente, "Compliance Is Your Floor, Not Your Ceiling: GRC Platforms Move To Value Creation," Forrester Blogs, March 9, 2020 (https://go.forrester.com/blogs/compliance-is-your-floor-not-your-ceiling-grc-platforms-move-to-value-creation/).

[12] Source: Margarita Hakobyan, "How Customers See Cybersecurity and Privacy Risks," CustomerThink, May 11, 2020 (https://customerthink.com/how-customers-see-cybersecurity-and-privacy-risks/).

[13] To help S&R professionals navigate the complex landscape of privacy laws around the world, Forrester created the data privacy heat map, which explains the data protection guidelines and practices for 61 countries. It also covers government surveillance, cross-border data transfers, regulatory enforcement, and data center locations around the globe. Due to the dynamic nature of data protection legislation, we update the interactive tool whenever there are significant changes to relevant legislation. We also conduct an annual comprehensive review and update. See the Forrester report "Forrester's Global Map Of Privacy Rights And Regulations, 2019."

[14] In our 33-criteria evaluation of risk-based authentication (RBA) providers, we identified the seven most significant ones — AppGate, IBM, Kount, LexisNexis Risk Solutions, OneSpan, RSA, and TransUnion — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk (S&R) professionals make the right choice. See the Forrester report "The Forrester Wave™: Risk-Based Authentication, Q2 2020."

[15] Source: Michael Moeser, "5 ways biometrics are going mainstream for payments," PaymentsSource (https://www.paymentssource.com/list/5-ways-biometrics-are-going-mainstream-for-payments).

FORRESTER® forrester.com

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

PRODUCTS AND SERVICES

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

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO

B2B Marketing

B2C Marketing

Customer Experience

Customer Insights

eBusiness & Channel Strategy

Technology Management Professionals

› CIO

Application Development & Delivery

Enterprise Architecture

Infrastructure & Operations

Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.