Top Research For CIOs: Security

Realize The Value That Excellent Security Delivers

by Matthew Guarini
March 15, 2019

Why Read This Report

Security no longer lives exclusively in the IT department. Now, thanks to ever-escalating attacks, boards and C-suites have become all too familiar with the risks of breaches, and they demand frequent updates of the firm's security posture. And more progressive companies are realizing that security can be an asset. This report gives CIOs insight into the trends, key issues, and opportunities to improve how security is managed regardless of whether you own the security function.

Key Takeaways

Applications Are The Primary Attack Vector For External Attacks

Cybercriminals are targeting your customer-facing and critical applications using direct attacks or by exploiting vulnerabilities. In addition, they'll continue to use phishing and other social engineering to use your own people and partners against you.

Use Security Maturity To Improve Your Investment Planning

CIOs spend many hours wondering which projects generate the most value for their organization and how best to allocate their security budget. A good approach is to plan, sequence, and explain the value of security investments based on how they will affect the maturity of your security program.

The Wider Technology Services Trend Comes To Security

Services have been among the fastest growing segments of tech spend for the past five years. 2018 saw security move in the same direction as services spend and surpass security product spend for the first time. These collaborations will lead to new ecosystems that drive value and reduce risk, mirroring the broader tech market.

Top Research For CIOs: Security

Realize The Value That Excellent Security Delivers

by Matthew Guarini
with Stephanie Balaouras, Sharyn Leaver, and Alyssa Danilow
March 15, 2019

Ubiquitous Tech Elevates Security And The Role Of The CIO

From the device in your pocket to your car to the voice assistant in your house, we are becoming more connected and dependent on technology. With the rise of technology dependence comes the inexorable rise of security challenges — and we are barely keeping up. In the last few months, Marriott suffered a mega data breach of 500 million accounts and the posting of more than 1 billion email and password combinations to an easy-to-access hacking forum.[1] In our Predictions 2019: Cybersecurity report, we predict that attackers will use automation to more effectively attack specific industries. To survive and thrive in today's global economy, it is critical that CIOs can identify and mitigate the cybersecurity risks to the firm's top business, financial, and operational initiatives. We have segmented breaches into four major categories, and as CIO, you must identify your biggest threats and prepare to combat them, regardless of whether the CISO reports to you, the CEO, or directly to the board (see Figure 1). It isn't easy, and it won't get easier. But you must provide security for your customers' and your company's information, or you won't have either for long.

The following research will help CIOs better understand some of today's most critical security threats, better prepare to allocate their security budget, and better communicate the firm's security posture to the board. For a full Forrester framework to help CIOs secure their customers, protect their brand, and drive differentiation, we recommend our cybersecurity and privacy playbook.

1. Top Cybersecurity Threats In 2019

Using finite budgets to protect their business from every possible attack type in the threat landscape is a challenge for CIOs. One strategy is to work with your security team to note historical attack trends, and after determining the most highly probable to occur in the future, prioritize attack protections. This report analyzes common attack trends responsible for breaches in 2018 to facilitate this approach. Some key insights that CIOs should understand about these threats include:

- **Direct web application attacks and software vulnerabilities are primary attack vectors.** Web application attacks and exploitation of software vulnerabilities continue to be the leading methods of external attack. CIOs need to find other ways to evaluate their organization's ability to develop secure code and support development to improve code quality.

FORRESTER®

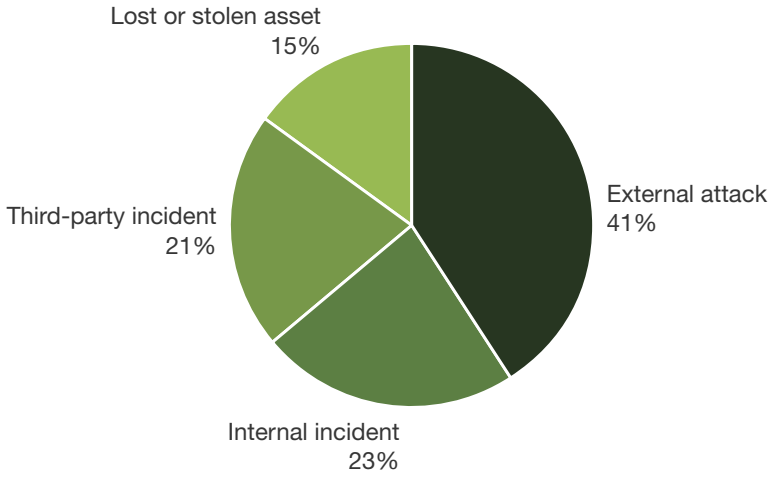
Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

- **Threat actors will compromise insiders and third parties.** It's critical to understand the ways threat actors engage insiders and third parties as proxies to attack your organization. Often, the real adversary is standing behind the people moving against your organization, making it difficult to assess risk based on specific actor capabilities.
- **Mobile malware is about to get terrifying.** In 2018, we saw a malware campaign preloaded on devices that had the ability to evolve based on interactions with a command and control system. Threat actors have noticed the amount of time we spend on our phones.

Read the report by Josh Zelonis: Top Cybersecurity Threats In 2019.

FIGURE 1 Major Causes Of Breaches In The Past 12 Months

"Which of the following categories did the breach(es) you experienced fall into?"



54% of respondents attributed their internal attacks to malicious intent, **38% to inadvertent misuse**, and **8% to a combination of the two.**

37% of respondents attributed their external attacks to web application exploits, **35% to software vulnerabilities**, and **27% to stolen credentials.**

Base: 101 to 180 network security decision makers at firms (1,000+ employees) that experienced a breach in the past 12 months
Source: Forrester Analytics Global Business Technographics® Security Survey, 2018

2. Security Budgets 2019: The Year Of Services Arrives

This report compares the budgets of global security decision makers at firms spending up to 10%, 11% to 20%, and 21% to 30% of their IT budget on information security. CIOs can use these budget ranges as a starting point to evaluate their team's programs, then compare their product, service, staffing, and other allocations with those of similar firms. Our key findings include:

- **Crucial industries need to step up security spending.** Key industries that handle massive amounts of personal data — financial services, insurance, public sector, and healthcare — are not spending enough on information security.
- **Services overtook products in 2018.** 2018 was the first year that saw spending on security services overtake spending on security products in every spending bracket. With the state of the security labor market on a growth trajectory, this will likely continue to be a trend in years to come.

Read the report by Jeff Pollard: Security Budgets 2019: The Year Of Services Arrives.

3. Justify Security Budget By Its Impact On Maturity

CIOs face challenges articulating which projects generate the most value for their organization. They often struggle to justify existing budgets, as well. To help you build the business case for new projects and justify existing funding, this report explains a unified way to plan, sequence, and explain the value of security investments based on their impact on your program's maturity. CIOs can use the insights in this report to understand and make the case for investing in security to improve the maturity of his or her enterprise:

- **Security maturity is the best way to gauge investment.** Improving maturity requires you to coordinate, scale, and optimize components of your security program. A high level of maturity indicates a security team that's aligned to the business and committed to measuring and optimizing its performance.
- **Maturity measures what's in your control.** Security teams spend too much time measuring their performance based on uncontrollable external factors — threat actors, tool sets, and motivations. Measuring maturity instead turns your attention to components you can control and for which you can define success.
- **Avoid wasting money with the impact on security maturity calculator.** Forrester's Impact On Security Maturity calculator will help you identify ways to optimize your security budget. If removing a current expense does not lower maturity, continuing to fund it is wasted money. This approach helps your analyze expenses by the outcomes they produce, not simply how they compare to other costs.

Read the report by Jeff Pollard: Justify Security Budget By Its Impact On Maturity.

4. How To Talk To Your Board About Cybersecurity

Whether there to answer questions, give a status update, or build support, CISOs need to make the most out of each opportunity they get in front of their board of directors. This report details what issues matter most to corporate directors and what CISOs need to do to effectively communicate with them. It also provides a PowerPoint template for a board-level cybersecurity presentation with suggestions on how to frame key topics for such a senior audience. For CIOs, regardless of whether the CISO reports to you, it is important to understand these issues so you can properly align your strategy with the security teams. Our key findings include:

- **CISOs must have direct access to the board.** CISOs whose immediate supervisors control access to board interactions risk leaving the board uninformed — or worse yet, misinformed — about the performance, accomplishments, and concerns of the cybersecurity program. CIOs must make sure that the board hears about security from the person charged with running it.
- **Consistent content and language win with the board.** CISOs and boards often find themselves at an impasse, talking about similar concepts in different ways. CIOs should work with theirs CISOs to make sure they are structuring their content with descriptive visuals and consistent vocabulary. This will maximize understanding and avoid the need to renegotiate what words mean and what graphics illustrate at every session.

Read the report by Jeff Pollard, Jinan Budge, and Paul McKay: How To Talk To Your Board About Cybersecurity.

5. The Forrester Tech Tide™: Zero Trust Threat Detection And Response, Q1 2019

Zero Trust threat detection and response technologies are increasingly critical to securing customers and protecting the firm's brand. To accelerate their performance in threat detection and response, companies are evaluating and adopting a range of contributing technologies. This Forrester Tech Tide™ report presents an analysis of the maturity and business value of the 18 technology categories that support Zero Trust threat detection and response. CIOs should read this report to shape their firm's investment approach to these technologies. Key insights include:

- **Choose the right solutions to improve speed of detection.** The less time an attacker has access to your environment, the less damage they will be able to do. Find the right technologies and services to find the attackers in your environment long before traditional security tools ring the alarm.
- **Integrated solutions prove strong business value.** Point products that have moved to integrated solutions like endpoint detection and response and endpoint security suites prove strong business value. Look for point products from the Experiment and Invest quadrants to follow.
- **The future demands automated discovery, configuration, and response.** CIOs are faced with an ever-increasing scale problem as the types of attacks, size of attacks, and technology to protect

are all expanding. Zero Trust threat detection and response technologies will respond by including features such as automated discovery, configuration, and response to lighten the burden.

Read the report by Josh Zelonis and Joseph Blankenship: The Forrester Tech Tide™: Zero Trust Threat Detection And Response, Q1 2019.

6. Quantum Is Not An Immediate Security Threat

Headline-grabbing statements about the near-term threat of quantum computers to security contain truth that is often disguised by hype. This report separates fact from fiction. CIOs need this information to help their business understand the real threat and prepare for a technology that is distant but accelerating. Our key findings include:

- **Quantum computers could eventually break today's encryption.** There is truth in the claim that quantum computers could someday break encryption. Asymmetric schemes like public key infrastructure (PKI) are the most vulnerable.
- **It will be 10 to 20 years before this happens.** Quantum computers need to solve steep engineering challenges like qubit error-correction. Experts think it will take 10 years or more before today's encryption is threatened. In the meantime, new quantum-safe schemes are evolving.
- **Quantum computing will change the security landscape.** The future will see a race between increasingly powerful quantum computers and new encryption schemes to secure data. You need to start by arming your team with knowledge.

Read the report by Brian Hopkins: Quantum Is Not An Immediate Security Threat.

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.

Endnotes

[1] Source: Kate O'Flaherty, "Collection 1 Breach -- How To Find Out If Your Password Has Been Stolen," Forbes, January 17, 2019 (https://www.forbes.com/sites/kateoflahertyuk/2019/01/17/collection-1-breach-how-to-find-out-if-your-password-has-been-stolen/#1a58f2572a2e).

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.

Packet Fusion

Ellen Pensky
ellen@bumblebeemarketing.net