NYSE

NYSE Governance Services

A 2015 SURVEY

Cybersecurity in the Boardroom

VERACODE

Following the slew of major cyberattacks reported in 2014—the Year of the Breach, according to *Forbes*—cybersecurity has become a boardroom-level conversation on an unprecedented scale.

The resignation of Target's CEO and CIO following that company's breach shows that responsibility is no longer being placed solely upon the CISO, but rather across the entire C-suite. In addition, high-profile vulnerabilities such as Heartbleed and Shellshock illustrate how much businesses rely on widely used open-source and third-party software components that have not been properly vetted for security. Yet there has been little visibility into the role the board is playing in addressing cybersecurity risk for companies.

To that end, NYSE Governance Services, in partnership with Veracode, surveyed nearly 200 directors of public companies representing a variety of industries—including financial services, technology, and health care—to discover how they view cybersecurity in the boardroom. Our goal was to gain insight into how cybersecurity is being understood, prioritized, and addressed at the board level.

Directors lack confidence in their companies' ability to thwart an attack and are increasingly holding the CEO and, in some cases, the entire executive team responsible in the event of a breach.

Two-thirds (66%) of the directors we surveyed are less than confident their companies are properly secured against cyberattacks. Given the large-scale breaches that have occurred at major corporations such as Sony, Target, JPMorgan Chase, and Anthem (among many others), it's not surprising that only 4% of respondents indicated they are "very confident" that their companies are properly secured against attacks.

More than 80% of those surveyed did say cybersecurity topics are discussed at nearly every meeting—yet alarmingly, one in five indicated they are only discussed after an internal incident or one in the same industry.

When a breach does occur, our results show boards are more likely to hold the CEO accountable. The CIO was most often chosen as the second-most responsible. This makes it apparent that responsibility for attacks is being seen as a broader business issue, signaling a shift away from putting the onus squarely on the chief information security officer (CISO) and the IT security team.

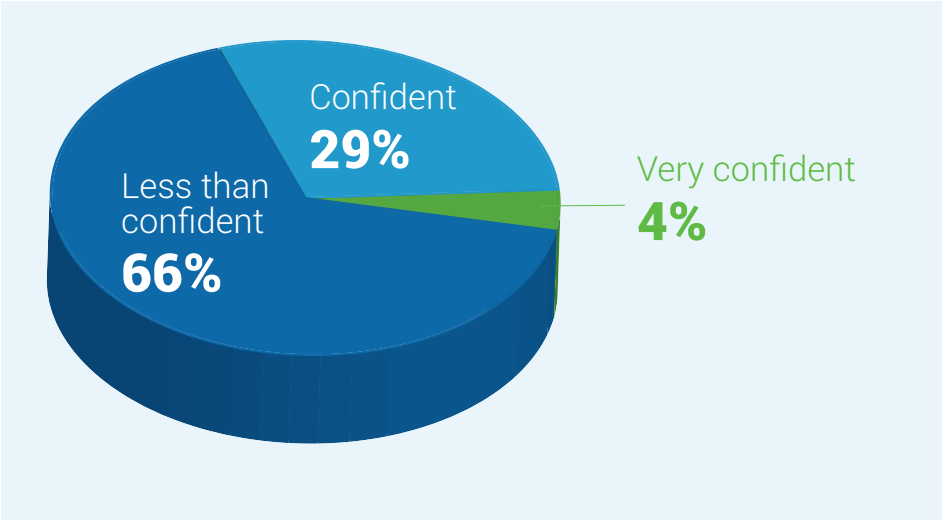
Brand damage, corporate espionage, and breach costs are directors' top three concerns.

When asked to rank their biggest cybersecurity fears, 41% of directors said they are most worried about brand damage. Another 47% are nearly equally split between concern over theft of corporate intellectual property (such as strategic plans and proprietary designs)—leading to a loss of competitive advantage—and the total cost of responding to a breach (including cleanup, lawsuits, forensics, and credit reporting costs).

In their comments, directors named specific worries such as the risk of

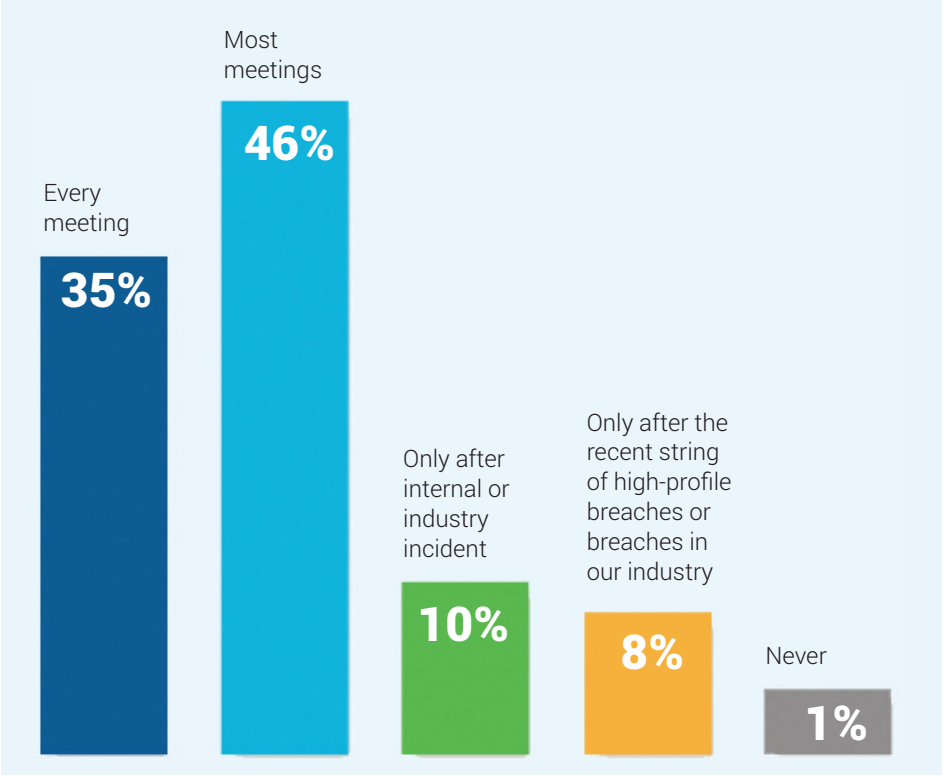
Cybersecurity

How confident are you that your companies are properly secured against cyberattacks?



IT Security

How often are cybersecurity matters discussed during board meetings?



business interruption, destruction of data, infrastructure damage, and follow-on attacks, including fraud perpetrated on individual customers.

One director expressed another type of worry, writing that he was concerned cyberattackers would subvert the company's devices to make them perform "in some way other than their intended fashion" —which would be particularly concerning in industries such as medical devices and automotive safety equipment.

While directors care about cybersecurity, they don't seem to understand how risk is introduced from the products and services they bring to market.

While directors are now prioritizing cybersecurity risk in boardroom conversations, they ranked security risks second to last in their list of concerns when introducing a new product or service to the market (after other criteria including revenue potential, competitive differentiation, and development costs).

"The more you increase security, the less user friendly" the product becomes.

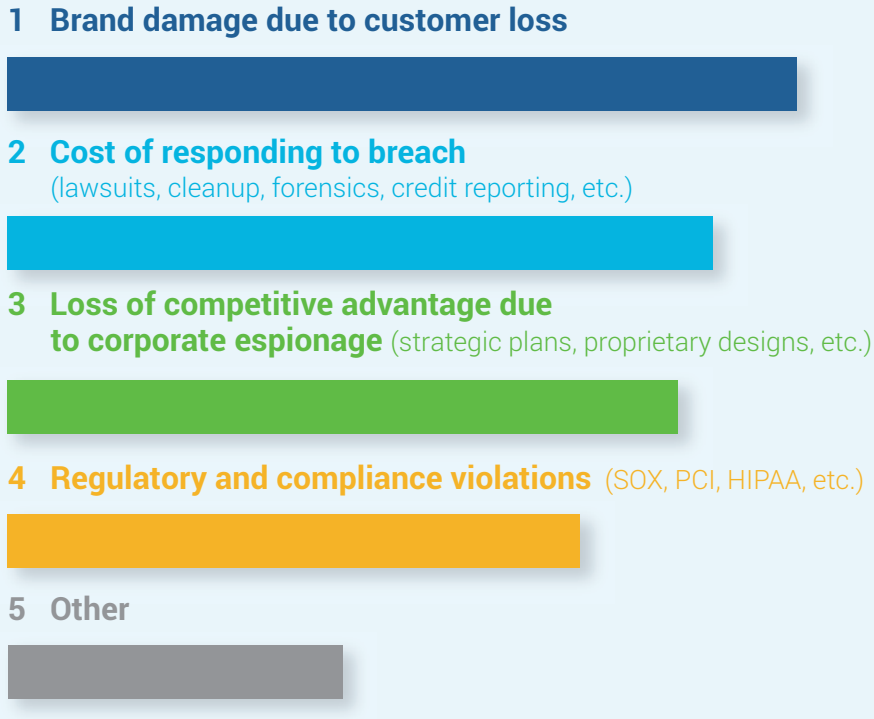
This appears to be an important disconnect, especially because more than half mentioned the ability to leverage new technologies such as cloud and mobile applications as a key barrier to keeping up with the pace of innovation. As one director stated, "The more you increase security, the less user friendly" the product becomes.

Accountability

Who do you hold accountable when a major breach occurs at your company?

Cyberattacks

What is your biggest fear regarding cyberattacks?



This reflects a common reluctance to add more security (such as requiring stronger passwords or two-factor authentication) because of the perceived inconvenience on the part of customers and partners. One clue to the disconnect with respect to priorities might be board member perceptions about how thoroughly their company's software products and services are assessed for vulnerabilities before being deployed. More than two-thirds of respondents believe that most or all of their web and mobile applications are assessed for threats before being made available to customers—yet separate studies by SANS and IDG Research show the majority of software applications produced by enterprises are *never* assessed for vulnerabilities (62%, according to IDG Research[1]).

Third-party software and supply chain risk are of substantial concern.

More than 70% of those surveyed indicated they have significant concerns about risk from third-party software in their supply chains. This is not surprising given recent high-profile breaches involving third parties[2] and increased attention on third-party risk by regulators.[3]

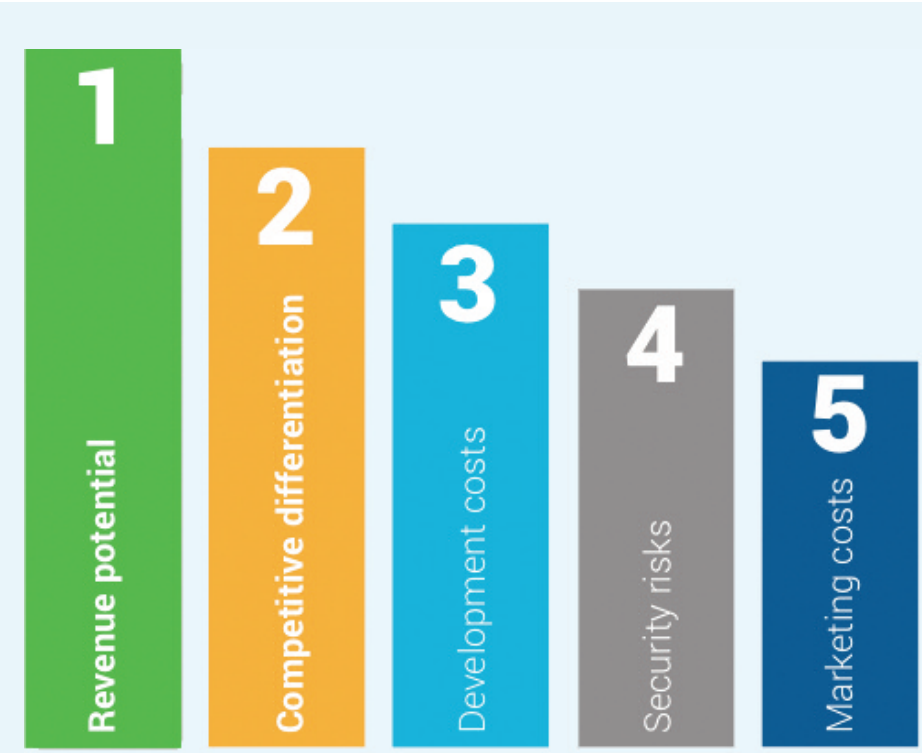
In addition, one director commented on a related third-party risk regarding the "inability to know whether customers and suppliers who use our systems have adequately secured their own access points."

CISOs can become more effective leaders in the boardroom.

While the pressure resulting from a breach might have shifted from the CISO to the CEO, in terms of

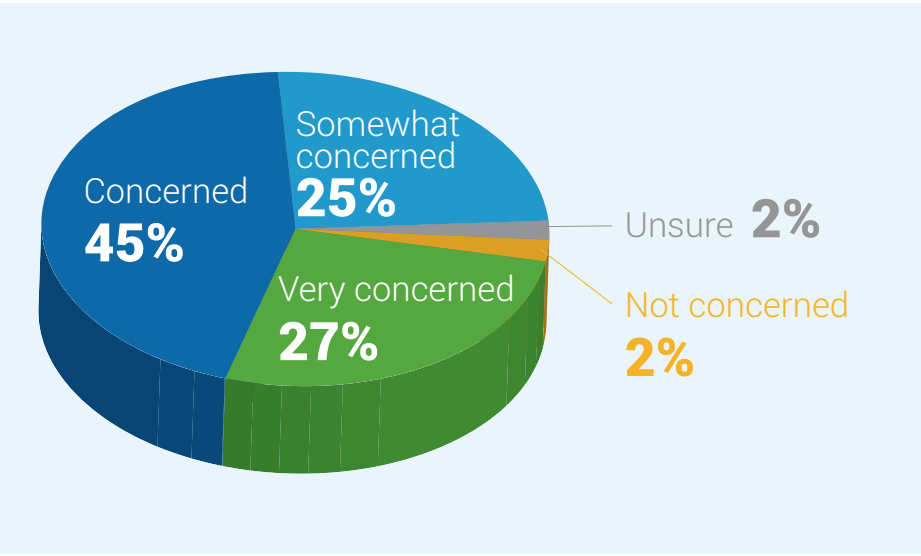
Technology

When introducing new technology-based products and services to the market, what are your top concerns?



Third-Party Software

How concerned are you about the risk from third-party vendor software?



[1] *https://info.veracode.com/whitepaper-idg-study-why-application-security-is-a-business-imperative.html*
[2] *www.wsj.com/articles/j-p-morgan-found-hackers-after-finding-breach-of-race-website-1414766443*
[3] *www.nytimes.com/2015/04/09/business/dealbook/wall-st-is-told-to-tighten-digital-security-of-partners.html*

accountability to the board, survey results show the CISO can take practical steps to become a more effective communicator.

When asked how they would like cybersecurity information to be presented, nearly two-thirds of respondents indicated a strong preference for either risk metrics or high-level strategy descriptions. It's clear that CISOs should be speaking to the board in terms directors understand, such as by using risk benchmarks compared to industry peers and talking about breaches in similar industries—rather than by describing specific security technologies.[4] Otherwise, CISOs run the risk of being seen simply as technologists rather than strategic business executives.

Accordingly, boards are looking for a combination of business and technology skills in their CISOs. While technical skills and experience were ranked as the key quality that directors value most in a CISO by a majority of respondents, business acumen and communication skills were seen as the second and third most valued qualities.

Leveraging new technologies, finding and hiring the right people, and ensuring the security of new products and services are the three biggest barriers to innovation.

Nearly three-fourths (72%) of those surveyed said that finding and hiring people with the right skills is the largest roadblock to keeping up with the pace of innovation. Almost 60% of respondents added that the ability to

CISO Qualities

What do you see as the key qualities of a chief information security officer (CISO)?

1. Technical skills and experience
2. Business acumen
3. Strong communicator
4. Risk taker
5. Crisis communication expert

IT Security

How do you prefer information regarding cybersecurity be presented?

[4] *https://info.veracode.com/whitepaper-forrester-ciso-2018-report.html*

leverage key technologies (including cloud, mobile, and analytics) also plays a primary role, while close to half (43%) are concerned about ensuring the security of new products and services.

Conclusion

While our results show that most boards are taking cybersecurity seriously, many directors aren't confident their companies have sufficient controls in place to defend against cyberattacks that are continuously being mounted by cybercriminals, nation-states, competitors, and hacktivists.

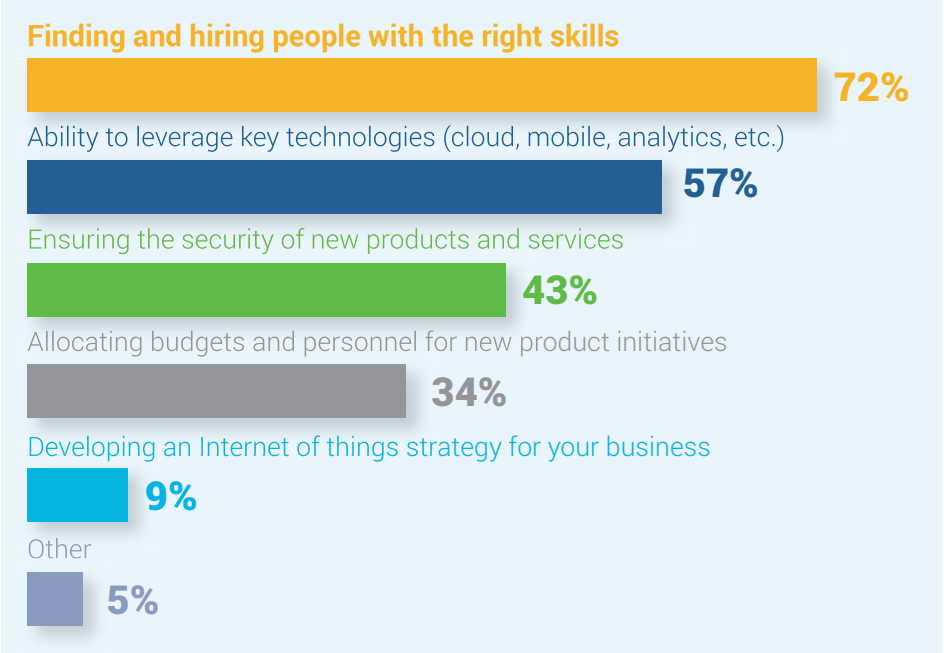
When a breach does occur, boards are increasingly looking to the CEO and other members of the executive team to step up and take responsibility. Directors are most concerned about reputational damage to the brand post-attack, yet cybersecurity is a fairly low priority when developing new products. Third-party/software supply chain risk is a significant concern. Accordingly, finding the right balance between innovation and risk when developing new products and services is still a work in progress.

Finally, CISOs need to combine their strong technical skills with solid business and communication skills in order to convey security information to the board in terms directors will understand.

We hope these key points and others drawn from the data in this report will form the basis for a comprehensive guide for CISOs when interacting with their boards—thus helping them become more effective corporate leaders. We also hope it will be beneficial for directors who are looking to bring more visibility and clarity about their companies' risk postures to their interactions with executive management teams.

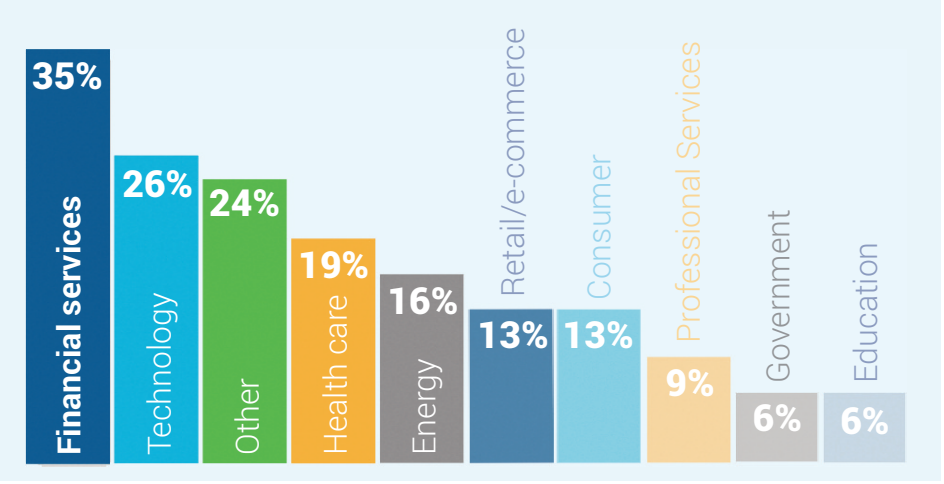
Innovation

What are the key barriers to keeping up with the pace of innovation?



Respondents

Which industries do you serve in as a board member?



Respondents

What is the primary role/position within the largest company on which you sit as a board member? How many boards do you sit on?

Primary role/position		Boards	
78%	Outside director	31%	One
12%	CEO	35%	Two
8%	Other	21%	Three
1%	Investor	8%	Four
1%	Co-founder	5%	Five or more

NYSE Governance Services

NYSE Governance Services

NYSE Governance Services is an integrated suite of resources for public and privately held companies worldwide seeking to create a leadership advantage through corporate governance, risk, ethics, and compliance practices. NYSE Governance Services leverages the expertise of Corpedia®, a leader in risk assessment and e-learning for ethics and compliance, and Corporate Board Member®, a trusted source on governance matters for company directors and C-level executives at both NYSE and Nasdaq companies. NYSE Governance Services offers a range of training programs, advisory services, benchmarking analysis and scorecards, exclusive access to peer-to-peer events, and thought leadership on key governance topics for company directors and C-level executives. **nyse.com/governance**

VERACODE

Veracode is a leader in securing web, mobile, and third-party applications for the world's largest global enterprises. By enabling organizations to rapidly identify and remediate application-layer threats before cyberattackers can exploit them, Veracode helps enterprises speed their innovations to market—without compromising security. Veracode's powerful cloud-based platform, deep security expertise, and systematic, policy-based approach provide enterprises with a simpler and more scalable way to reduce application-layer risk across their global software infrastructures. Veracode serves hundreds of customers across a wide range of industries, including nearly one-third of the Fortune 100, three of the top four U.S. commercial banks, and more than 20 of Forbes' 100 Most Valuable Brands. Learn more at www.veracode.com, on the Veracode blog, and on Twitter.