Cybersecurity Perspectives 2018

THE DATA BREACH EFFECT

SCALE
Venture Partners

Table of Contents

SCALE Venture Partners

Introduction

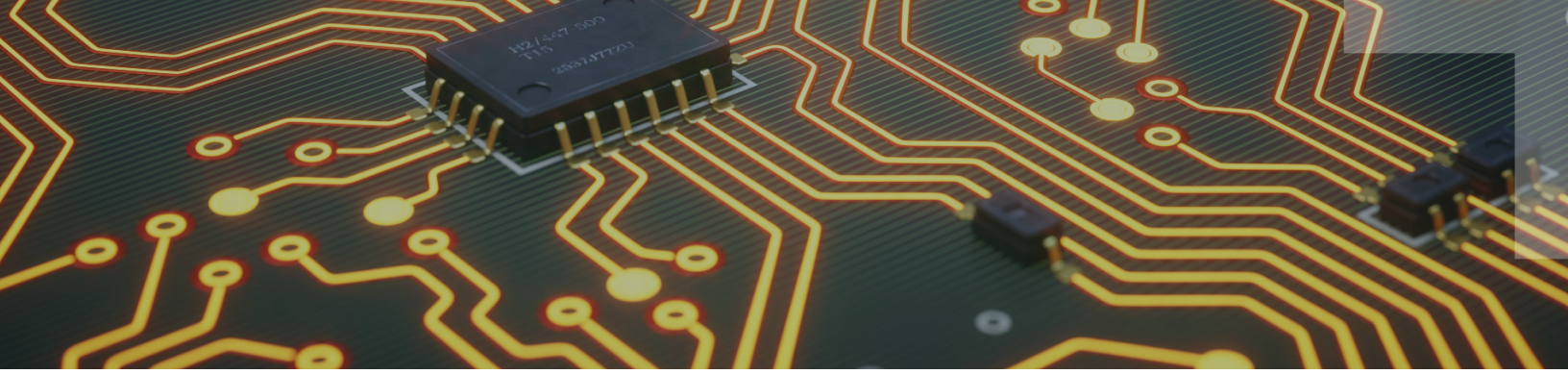
On March 2, 2018, Equifax provided updates related to its 2017 breach that exposed social security numbers and other sensitive information of millions of consumers. The company disclosed that an additional 2.4 million people had been affected by the breach, bringing the total to 147.9 million, and that costs related to the incident would likely exceed $600 million.

Yahoo, which had reported two big breaches in 2016, disclosed in 2017 that all 3 billion of its user accounts had been affected, double the previous estimate. Like other cyber attacks, damage from breaches can carry on long after the incident appears to be over.

Every year, cybersecurity threats become more pervasive and menacing. Businesses struggle to stay ahead of hackers as breaches grow in frequency and scope, and are made public due to disclosure laws. The list of breaches disclosed in 2017 is long, ranging from HBO and Verizon to the U.S. Securities and Exchange Commission and the Republican National Committee's marketing firm. According to a report from the Identity Theft Resource Center, there were a record number of breaches in 2017 (1,579), up nearly 45 percent from the year before.

These breaches are influencing how executives think about security and their approaches to protecting their company networks and their customer data. The risk is too great — damage to corporate brand and reputation, loss of consumer confidence and financial penalties, as well as lawsuits and firings. We surveyed top professionals, from directors to C-level executives, about their thoughts and plans in the aftermath of the cybersecurity incidents in 2017.

In our latest annual report, "Cybersecurity Perspectives 2018: The Data Breach Effect," we examine how these perceptions and actions have changed in the past year. To summarize, security leaders are making changes to put themselves in a better position to address cyber threats and minimize risk. As a result, they are generally more confident that they are equipped to handle most threats, although breaches remain a high-level concern. However, outdated security processes and technology pose serious challenges for security teams, who are struggling to stay ahead of hackers. Furthermore, there seems to be a disconnect between directors and the most senior executives in their perceptions of certain cyber risks and their ability to manage them. These internal issues could ultimately undermine their ability to prevent and mitigate breaches.



Key Findings

SECURITY BREACHES DRIVE CHANGE

More than 90 percent of security executives said breaches led their organization's CEO or board to change their security programs in some way or another, most commonly through increased cybersecurity spend. The two biggest drivers of change in 2017 were high-profile breaches and the General Data Protection Regulation (GDPR) May 2018 deadline, which is pushing data privacy to the forefront of global companies with EU customers.

PRIVACY CONCERNS REMAIN

Executives are very concerned about privacy specifically, but feel relatively prepared to handle cyber risks generally. While data breach of sensitive information was perceived as the No. 1 security risk over the past two years, data privacy and lack of privacy controls are increasingly pressing concerns. Still, four out of five executives feel they are more equipped than they were a year ago to handle cybersecurity risks overall.

CLOUD INFRASTRUCTURE UPGRADES

Migration to the cloud remains a dominant factor for companies as they double down on infrastructure. As a result, security leaders' top security investment priorities for 2018 (as was the same for 2017 and 2016) remain cloud infrastructure security, cloud application security and network security.

TOP SECURITY CHALLENGES

The top challenges impacting security teams are too many alerts and false positives, and outdated technology and processes. These obstacles leave security teams at increased risk of missing indicators of a breach and unable to leverage new automated solutions that can help triage alerts and incidents. As a result, security teams aren't able to effectively identify and respond to real threats.

EXECUTIVE PERSPECTIVES VARY

There's a clear divide between the C-suite and directors when it comes to views on top risk factors, threat preparedness and accountability for security. C-level executives place ultimate responsibility on the C-suite (namely, CIOs and CEOs), while directors view the IT department as ultimately accountable. Meanwhile, C-level executives are more optimistic about the ability to manage specific threats than directors.

Big Breaches Force Change

From increasing the security budget to greater board and CEO involvement in security planning, companies are beefing up security in the wake of high-profile breaches.

The Equifax breach was unprecedented in severity and scope, exposing the highly sensitive data of most Americans and creating a long-tail fallout. In March 2018, the company announced that even more data was exposed than originally reported — affecting nearly 150 million people. The breach means people will have to monitor for identity theft for the remainder of their lives. As a result, executives held accountable for breaches now risk losing their jobs, just as three Equifax executives did. Additionally, a proposed bill in the U.S. Senate could land executives in jail for not disclosing a breach. The fallout surrounding high-profile breaches has had a ripple effect on how executives now think about and manage security. Nearly 70 percent say they are now spending more on new security technologies and 60 percent upped their security budget, while more than half increased the size of their security teams.

OF SECURITY PROFESSIONALS REPORT THAT THE EQUIFAX BREACH CHANGED THEIR PERSPECTIVES AROUND SECURITY

OF EXECUTIVES SAID THE MOST SENIOR SECURITY DECISION MAKER REPORTS DIRECTLY TO THE CEO AND ONE-QUARTER SAID THE CIO

OF RESPONDENTS SAID THAT THEIR CEO OR BOARD ENACTED CHANGES AS A RESULT OF FALLOUT FROM RECENT HIGH-PROFILE BREACHES, WITH NEARLY 50 PERCENT ALLOCATING GREATER BUDGET TO SECURITY AND INCREASING MEASUREMENT AND REPORTING AROUND SECURITY DECISIONS

OF SECURITY PROFESSIONALS REPORT THAT THE NEW SENATE BILL PROPOSING TO MAKE NON-DISCLOSURE OF A BREACH A JAILABLE OFFENCE CHANGED THEIR PERSPECTIVES AROUND SECURITY

WHAT CHANGES HAS YOUR ORGANIZATION MADE DUE TO HIGH-PROFILE BREACHES?

68%

INCREASED INVESTMENT IN NEW CYBERSECURITY TECHNOLOGIES

60%

GREATER BUDGET ALLOCATED TO SECURITY

55%

INCREASED INVESTMENT IN SECURITY PERSONNEL

49%

INCREASED MEASUREMENT AND REPORTING

38%

GREATER INVOLVEMENT BY THE CEO / BOARD IN SECURITY DECISIONS

Breaches, Hackers and Data Privacy Are Top Concerns

Executives are most worried about data breaches, though privacy controls are a fast growing concern as regulations and compliance pressures rise with the adoption of stricter EU rules.

Data breaches have been top of mind for executives over the past three years for obvious reasons. When asked to list their top three IT security risks, the No. 1 most commonly cited risk was data breach of sensitive information, followed by employee or user negligence and external attacks.[1] When asked what keeps them up at night with regard to protecting data, the top response for most executives was hackers, the same as last year.

With regard to protecting privacy, lack of data privacy controls went from third place in 2016 to the second spot in 2017.[2] New European Union privacy regulations set to go into effect in 2018 are no doubt weighing heavily on the minds of security leaders. Companies outside the EU, including the U.S., where consumer data privacy rules are more lax, are scrambling to figure out how to comply with the tougher EU rules. The regulations include penalties for not disclosing breaches within 72 hours.

TOP SECURITY RISKS IN 2017

DATA BREACH OF SENSITIVE INFORMATION **(60%)**

EMPLOYEE/USER NEGLIGENCE **(40%)**

EXTERNAL ATTACKS **(40%)**

REGARDING DATA PROTECTION, WHAT ARE THE TOP ISSUES THAT KEPT EXECUTIVES UP AT NIGHT IN 2016?

HACKERS **(46%)**

EMPLOYEE MISTAKES **(32%)**

LACK OF DATA PRIVACY CONTROLS **(30%)**

REGARDING DATA PROTECTION, WHAT ARE THE TOP ISSUES THAT KEPT EXECUTIVES UP AT NIGHT IN 2017?

HACKERS **(49%)**

LACK OF DATA PRIVACY CONTROLS **(46%)**

EMPLOYEE MISTAKES **(35%)**

1 Percentages in this section add up to 300 percent (not 100 percent) because respondents were asked to select their top three choices.

2 This survey was conducted in December 2017 and reflects sentiments and priorities for 2017 and into 2018. For all questions and responses concerning current risks and priorities, the year referenced is 2017.

Cloud Investments Remain Strong Now and Into Next Year

Cloud adoption — everything from infrastructure-as-a-service (IaaS) to application services (SaaS) and application infrastructure services (PaaS) — continues to grow in 2018, leading to increasing interest in cloud security.

A March 2018 McKinsey & Co. report found that enterprises expect to double their cloud adoption in the next three years, with 38 percent of their workloads in the public cloud, up from about 19 percent, partially as a result of improved cloud security.

Not surprisingly, cloud infrastructure was the No.1 investment by security leaders in 2017 (83 percent)[3] and 2016 (81 percent). Looking forward, executives say they plan to boost investment in cloud infrastructure and cloud application security, network security and data security / data loss prevention. Another trend is threat intelligence, which rose quickly as security teams look to invest in it in the future — jumping from 38 percent to 53 percent over the last year, although not yet a top priority. Organizations are realizing that security strategy can be even more effective with an understanding of the threat signals in the dark, deep and open web.

INVESTMENT IN THREAT INTELLIGENCE

38%

IN 2016

53%

IN 2017

53%

IN 2018 *(Projected)*

TOP TECHNOLOGY INVESTMENTS[4]

2016

- CLOUD SECURITY **(81%)**
- NETWORK SECURITY **(80%)**
- DATA CENTER / SERVER SECURITY **(75%)**
- DATA LOSS PREVENTION **(73%)**
- ENDPOINT SECURITY **(60%)**

2017

- CLOUD INFRASTRUCTURE SECURITY **(83%)**
- NETWORK SECURITY **(78%)**
- CLOUD APPLICATION SECURITY **(75%)**
- DATA CENTER / SERVER SECURITY **(72%)**
- DATA SECURITY / DATA LOSS PREVENTION **(65%)**

2018 *(Projected)*

- CLOUD INFRASTRUCTURE SECURITY **(73%)**
- CLOUD APPLICATION SECURITY **(69%)**
- NETWORK SECURITY **(65%)**
- DATA SECURITY / DATA LOSS PREVENTION **(61%)**
- DATA CENTER / SERVER SECURITY **(54%)**

[3] The 2017 report, which reflects survey responses from 2016, only included cloud security. However, the 2018 report, which reflects survey responses from 2017, broke the category out into two: cloud infrastructure security and cloud application security.

[4] Percentages in this section add up to 300 percent (not 100 percent) because respondents were asked to select their top three choices.

Excessive Alerts and Outdated Technology and Processes Pose Biggest Security Challenges

Security teams are drowning in security alerts and dealing with outmoded security, leaving them increasingly exposed to data breaches and other attacks.

With organizations increasing their investments in security, what's holding them back from improving their security posture? The volume of security alerts and/or false positives with detection software, along with antiquated security technologies or processes, are the two biggest obstacles for security organizations. In recent years, there has been an influx of detection tools that have crowded the market, all claiming to be the silver bullet for security. But these solutions have created an avalanche of alerts that security teams can't efficiently or effectively triage. This means that one crucial alert that signifies a breach could be buried beneath hundreds of notifications, and teams could find it too late or miss it altogether. They need a way to sift through alerts, eliminate false positives and find correlations between all the signals to identify the truly dangerous ones.

This is both a technology problem and a process problem. There are technologies available that allow teams to automate processes and be more efficient, but often the security organizations aren't at a level of maturity to make effective use of the automation. They may be relying on partly-manual processes still, or lack the necessary standardization and organization to use such tools. There is a big need for products that are targeted specifically at enabling security operations centers to be more effective in routine areas, such as alert vetting and analysis. This would have a significant impact on security teams that are overloaded by too high of a signal-to-noise ratio, which can mean the difference between becoming the next big data breach victim or stopping an attack in its tracks.

[5] Percentages in this graph add up to 300 percent (not 100 percent) because respondents were asked to select their top three obstacles.

TOP OBSTACLES HOLDING SECURITY ORGANIZATIONS BACK [5]

53%

TOO MANY ALERTS / FALSE POSITIVES WITH DETECTION SOFTWARE

53%

OUTDATED SECURITY TECHNOLOGY / PROCESSES

41%

NOT ENOUGH BUDGET

37%

COMPLEX LEGACY DATA CENTER INFRASTRUCTURE

31%

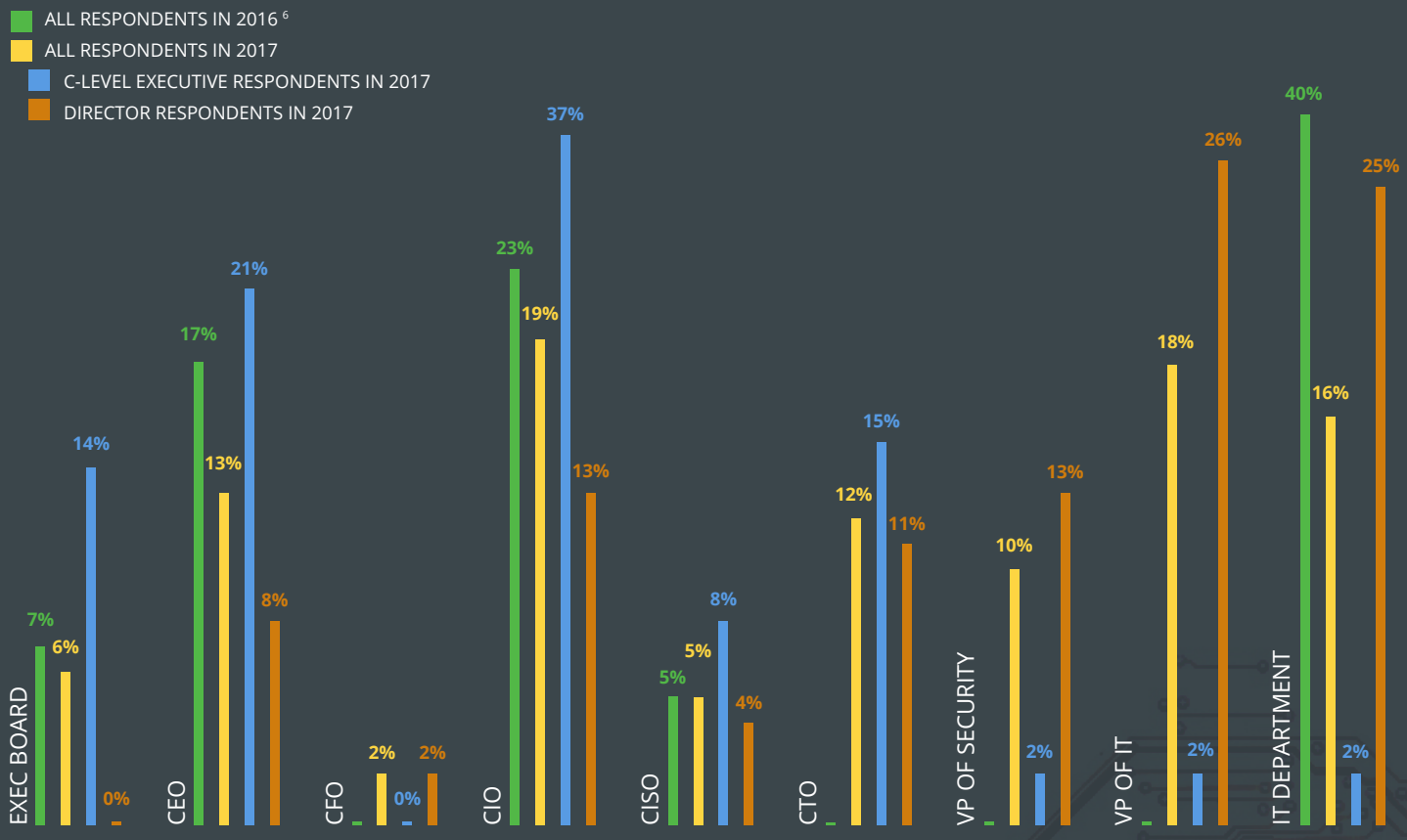
NO SOLUTIONS ON THE MARKET TO ADDRESS OUR NEEDS

There's Role-Based Misalignment on Accountability and Risk Drivers

From directors to VPs and C-level roles, executives are placing greater accountability for security problems on themselves.

Three out of four executives agree that leadership takes security very seriously (an increase from previous years), but not everyone agrees on who is ultimately responsible. Given that the CEO, CIO and CSO at Equifax lost their jobs as a result of the breach, the question of accountability is more important than ever before. Overall, most people believe that either the CIO, the VP of IT or the IT department (in that order) is ultimately responsible. That differs from the order of accountability last year, when most people placed the IT department at the top of the accountability chain, followed by the CIO. In breaking down the responses by job title, an interesting trend emerges: there's a divide between who C-levels and directors feel is ultimately responsible for the security of their organizations. C-level executives feel the C-suite should be held accountable whereas directors point further down the chain of command to VP and below in the IT department.

WHO IS ULTIMATELY ACCOUNTABLE FOR DATA SECURITY IN YOUR ORGANIZATION?



[6] In 2016 the C-suite was not broken down into smaller categories. The CEO & executive team was said to be 17% responsible for data security in organizations.

SCALE Venture Partners

There are rising levels of optimism going up the chain of command regarding specific risks and the company's ability to manage them.

Across the board, C-level executives are also more optimistic than directors about their company's ability to manage risks from a variety of threats. This could be due to the fact that directors are receiving frequent reports from security teams and are more entrenched in individual incidents, providing them greater visibility into security issues and deeper understanding of the risks. Or it could be that directors are putting greater emphasis on risks because security is a larger part of their job and thus more top of mind compared to the overall business risks that CEOs and other executives deal with.

When asked to compare how equipped they are now to deal with cybersecurity risks compared to a year ago, 80 percent said "much more" or "somewhat more" equipped. Nearly two-thirds ranked themselves highly equipped to handle cybersecurity risks (8 or above on a 1-10 scale), whereas a year ago just over half had the same positive outlook.

FEEL MORE EQUIPPED TO HANDLE CYBERSECURITY RISKS THAN 12 MONTHS AGO

88%

C-LEVEL

80%

ALL RESPONDENTS

FEEL VERY CONFIDENT IN THEIR COMPANY'S ABILITY TO HANDLE CYBERSECURITY RISKS (8 OR ABOVE ON A 1-10 SCALE)

61%

IN 2017

53%

IN 2016

CONFIDENCE IN COMPANY TO EFFECTIVELY MANAGE SECURITY RISKS

C-LEVEL EXECUTIVES
DIRECTORS

CRYPTO MINING
83% 64%

NON-COMPLIANCE
77% 64%

NATION-STATE & ESPIONAGE
73% 56%

MALWARE / ADVANCED PERSISTENT THREAT
83% 68%

DATA BREACH OF SENSITIVE INFORMATION
83% 68%

RANSOMWARE
71% 61%

EMPLOYEE OR USER NEGLIGENCE
73% 62%

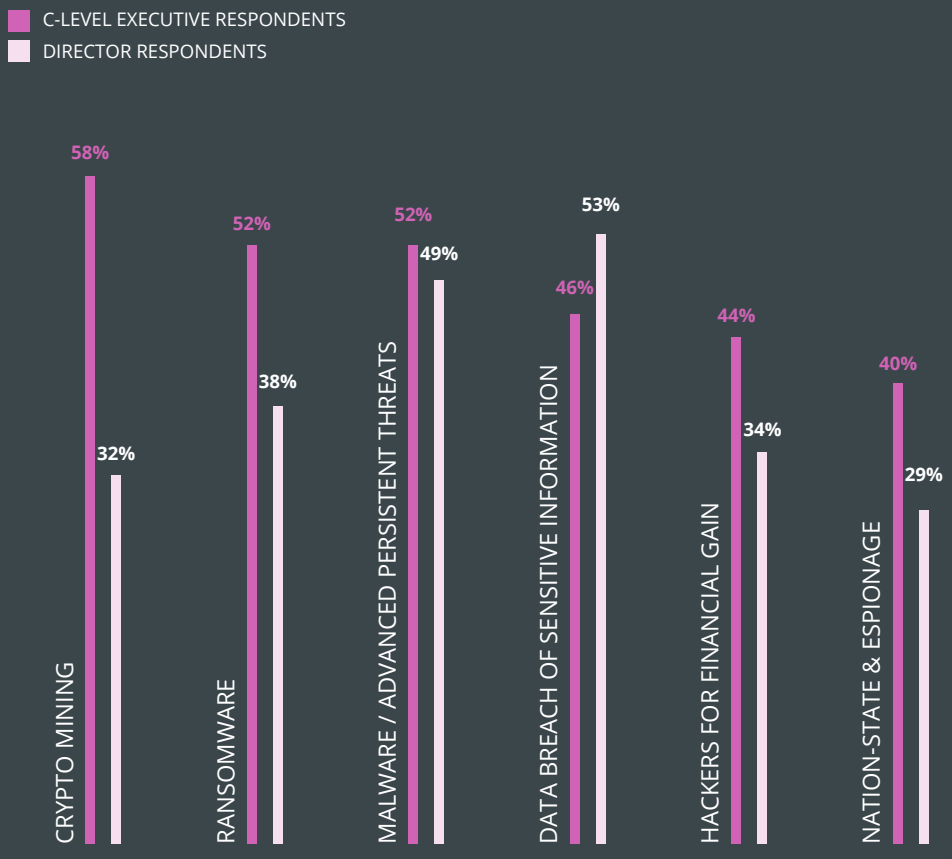
HACKERS FOR FINANCIAL GAIN
69% 57%

PHISHING ATTACKS
71% 64%

Aligning on potential risks is an opportunity for companies looking to protect themselves.

The type of risks concerning executives also vary depending on role. For example, directors view data breaches of sensitive information and malware as the two biggest concerns, while more senior executives name crypto mining and ransomware — relatively new threats that are gaining a lot of attention and mindshare with the public in news headlines. This misalignment is troubling — executives and their teams should be on the same page when it comes to security risks and priorities — and could be difficult to resolve. It's hard to address a security problem when it's not just a technology problem, but an organizational and cultural mismatch. Security professionals need to have clear communications with all stakeholders so that they can align on priorities, risks and accountability.

TOP SECURITY RISKS EXPECTED TO INCREASE IN 2018[7]



[7] Percentages in this graph add up to 300 percent (not 100 percent) because respondents were asked to select their top three choices.

Conclusion

The mega data breaches of recent years have begun to influence incremental but important shifts in attitude and action by security leaders. These breaches have become a forcing function for increased investment in security technologies and budget in general. What's more, new EU data privacy rules are pushing regulatory compliance for data protection to the forefront. And executives are giving more serious consideration to who is ultimately responsible for security at their companies.

There's also a divergence in opinion between directors and upper management about important security matters, in particular what they feel are the more pressing security risks facing their company and how prepared they are to handle them. This disconnect could result in greater exposure to risks and less of an ability to address them if executives aren't in agreement on the biggest threats and investments. There is an opportunity here for C-level executives and directors to strengthen internal communication and sync on cybersecurity issues. Executives throughout the organization need to be aligned on this in order to strengthen their security posture and protect sensitive data from hackers.

Escalating external threats, lack of internal agreement on security matters and reliance on outdated and inadequate technology are creating a perfect storm for businesses. More than ever, security teams need to be using technology that helps, not hinders, their jobs. Security professionals and executives up the chain need to have a common understanding of the security risks, a shared vision for how to address them and the processes in place to bring this vision to life. That entails making significant organizational and cultural changes, and fast. It won't be easy, but it's essential. It could be the difference between the companies that can weather the storm and those that capsize.

Methodology

Scale Venture Partners conducted a survey of 200 security leaders in the United States who are responsible for security buying decisions, the success of security deployments or the overall security of their company.