Cybersecurity Perspectives 2019

PREPAREDNESS BREEDS CONFIDENCE AMONG SECURITY LEADERS, DESPITE NOISY THREAT LANDSCAPE

SCALE
Venture Partners

Contents

Introduction

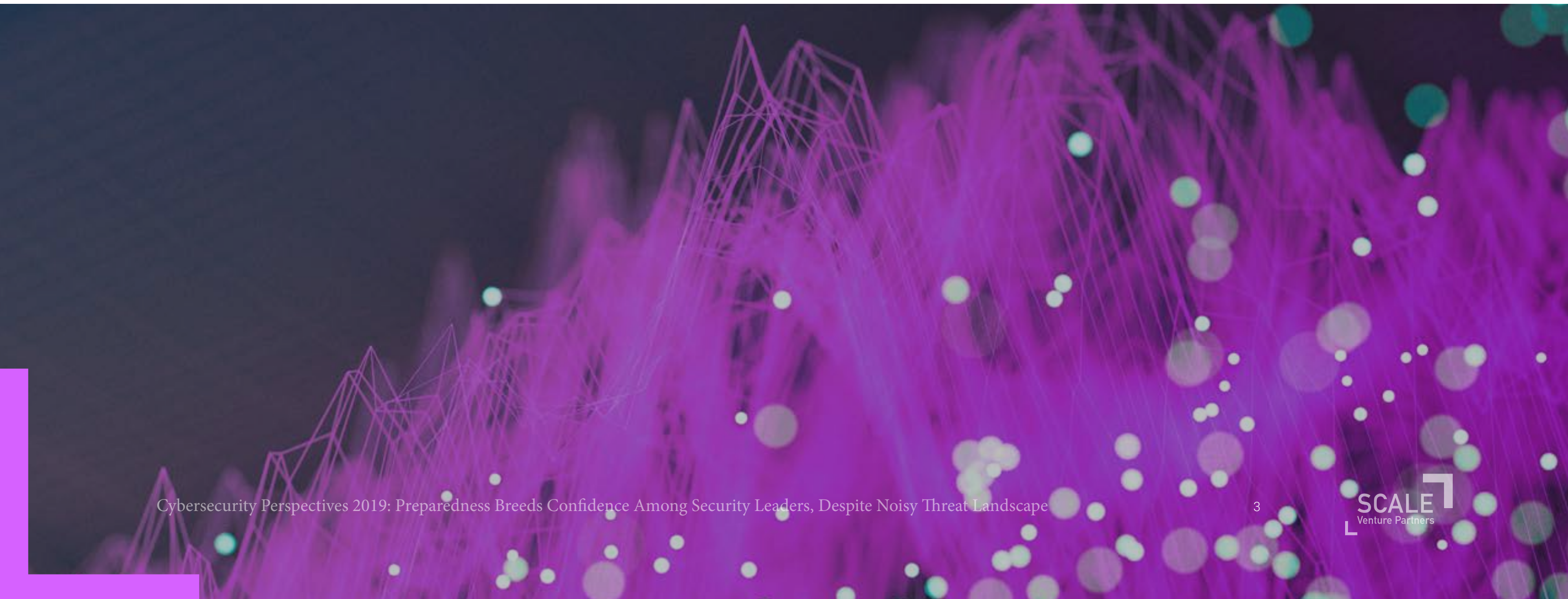
2018 marked a turning point for the cybersecurity industry, ushering in a new era of cyber accountability for business executives. Just under one year ago, the General Data Protection Regulation forced businesses worldwide to re-examine their accountability for their customers' personal data. Most recently, a settlement of a shareholder lawsuit against Yahoo in response to the company's mishandling of a series of data breaches paved the way for future lawsuits against executives at firms that experience major cyber attacks, regardless of the part they play in their organization's security strategies.

These events and others have presented companies with greater obstacles to managing security risks. In response to these concerns, a generation of cybersecurity vendors has brought new point solutions to the market with the help of mega funding rounds. In 2018, venture capitalists invested $5.3 billion in cybersecurity—nearly double that of 2016—to help businesses get a grip on their security posture. With so many solutions on the market, security professionals are confident that they're equipped to manage and mitigate risk.

At the same time, the threat landscape continues to evolve. Attacks are getting more sophisticated and the cost of an attack for victims is rising. A data breach now costs businesses $3.86 million on average and cybercrime is expected to cost businesses up to $6 trillion by 2021. Seemingly every day another attack makes headlines, and the number of consumers affected keeps hitting new records. In just the first month of 2019, researchers discovered hackers were freely distributing 2.2 billion stolen usernames and passwords on hacker forums.

With the number of attacks and victims rising, how are businesses feeling? Our survey found that, while executives have concerns about the risks facing their organizations, they feel more confident than ever that they're equipped to handle these risks. This indicates that the protocols and controls businesses have put in place as a result of major breaches and regulations like GDPR, the investments they've made, and the personnel they've hired have appeased some concerns around risk management. However, the threat landscape remains unchanged. If anything, it's worse than it's ever been.

In our latest annual report, "Cybersecurity Perspectives 2019: Preparedness Breeds Confidence Among Security Leaders, Despite Noisy Threat Landscape", we examine how perceptions and actions around cybersecurity investment and strategies have changed in the past year.



Key Findings

Security incidents prompt increased investment

Data breaches like data aggregator Exactis, data exposures like Cambridge Analytica, and regulations like GDPR forced organizations to reevaluate their approach to data privacy in 2018. Fifty-five percent of executives increased their investment in new data privacy solutions, 49 percent increased their measurement and reporting around data privacy, and 48 percent increased investment in data privacy personnel.

Businesses are approaching security holistically

Organizations now treat security as part of the entire business, rather than a siloed back-office function. Two-thirds of professionals say their organization has increased integration of security with other teams such as IT, operations and software development over the past year. Just 12 percent of executives say their IT security strategies are determined by budget and resource constraints, compared to 31 percent in 2017.

Executives feel prepared to handle security risks

Seventy-eight percent feel they are well equipped to handle cybersecurity risks, a 17 percent increase from 2017. The risks about which they feel most confident are data breaches (84 percent) and insider threats (83 percent). Eighty five percent of executives feel they are at least somewhat more equipped than they were a year ago to handle risks.

Threats stay top of mind for businesses

Data breaches of sensitive information, malware and advanced persistent threats, and hackers are the top three issues keeping executives up at night.

Legacy technologies remain an obstacle

While investments in new technologies are increasing confidence levels, old technologies continue to hold executives back. Over half of respondents think complex legacy data center infrastructure (53 percent) and outdated security technology and processes (52 percent) are the top obstacles holding their organization back from achieving the security posture it needs.

Security accountability rises to the C-suite

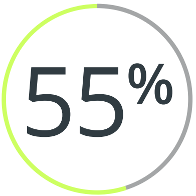
Fifty-eight percent of executives say a member of the C-suite is responsible for the security of their organization. Of the C-suite, CIOs took the lead at 20 percent.

Security Incidents Prompt Change

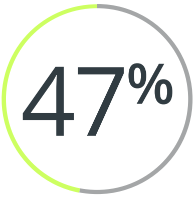
Data breaches like data aggregator Exactis, data exposures like Cambridge Analytica, and regulations like GDPR shook up the cybersecurity landscape in 2018, prompting businesses to elevate the importance of cybersecurity and increase investment in new security solutions.

Just over half (55 percent) of executives increased their investment in new solutions because of these incidents. Forty-nine percent increased their measurement and reporting around data privacy and 48 percent increased investment in data privacy personnel.

Cloud continues to take priority for 2019. When asked which security technologies and strategies they plan to invest in over the next 12 months, 60 percent of executives cite cloud application security and 58 percent cite cloud infrastructure security. Data privacy spending emerged quickly as a top area of spending in 2018 as the compliance deadline for GDPR caused a shift in how businesses approach their customer data.

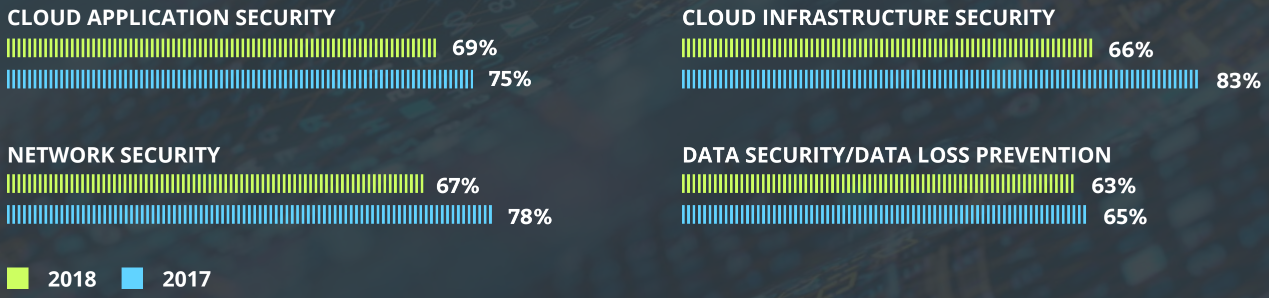


OF EXECUTIVES HAVE INCREASED INVESTMENT IN NEW DATA PRIVACY SOLUTIONS AS A RESULT OF DATA BREACHES



OF EXECUTIVES BELIEVE GDPR PROVIDES ADEQUATE GUIDANCE AND ENFORCEMENT TO ENSURE THAT BUSINESSES PROPERLY ADDRESS DATA PRIVACY ISSUES IN THE U.S.

TOP TECHNOLOGY INVESTMENTS IN 2018



TOP TECHNOLOGY INVESTMENT PRIORITIES PROJECTED FOR 2019

60%
CLOUD APPLICATION SECURITY

58%
CLOUD INFRASTRUCTURE SECURITY

49%
NETWORK SECURITY

48%
DATA SECURITY / DATA LOSS PREVENTION

47%
DATA CENTER / SERVER SECURITY

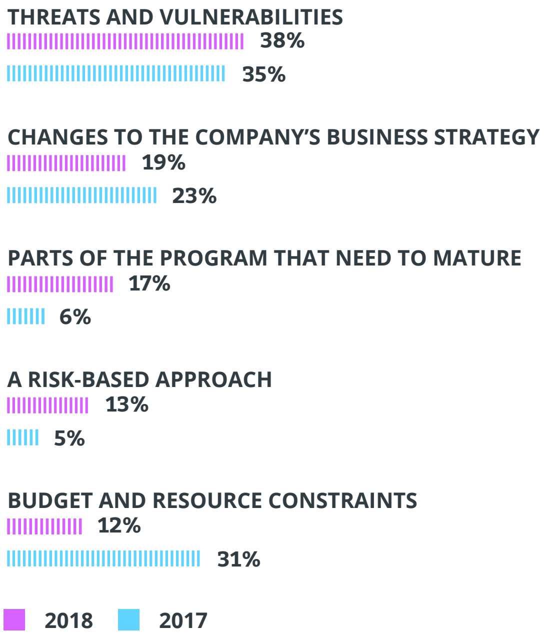
Organizations Adopt Holistic Approach to Security

Security is no longer a back-office function. Two-thirds of professionals (66 percent) report their companies have increased integration of security with other teams such as IT, operations, and software development over the past year.

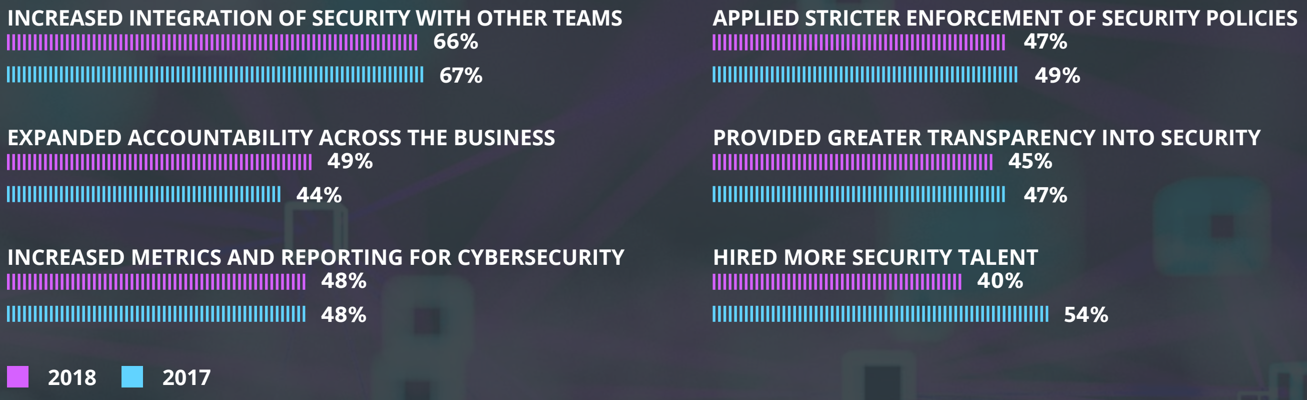
Though organizations report a diverse set of drivers for their IT security strategies, threats and vulnerabilities continue to reign (38 percent). Strategies determined by budget constraints, however, dropped from second place in 2017, at 31 percent, to last place in 2018, at 12 percent.

Just 40 percent of professionals hired more security talent over the last year. At last place, this was a steep decline from last year, when hiring came in second at 54 percent, suggesting organizations feel their hiring needs were met as a result of their investment focus in 2017.

TOP DRIVERS FOR IT SECURITY



EXECUTIVES CHANGED THEIR PROCESSES & STRATEGY AROUND SECURITY IN THE PAST 12 MONTHS



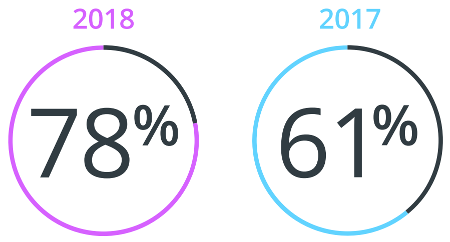
Confidence Skyrockets Despite Continuance of Threats

Despite attacks continuing to plague businesses, executives are more confident than ever before that they're equipped to effectively manage risk.

Cyber attacks are among the biggest risks in 2019 and are nearly as likely as natural disasters, according to the World Economic Forum. Yet, 78 percent of professionals feel they are well equipped to handle cybersecurity risks, a 17 percent increase from just a year ago. Eighty-five percent feel they are at least somewhat more equipped to handle risk than a year ago.

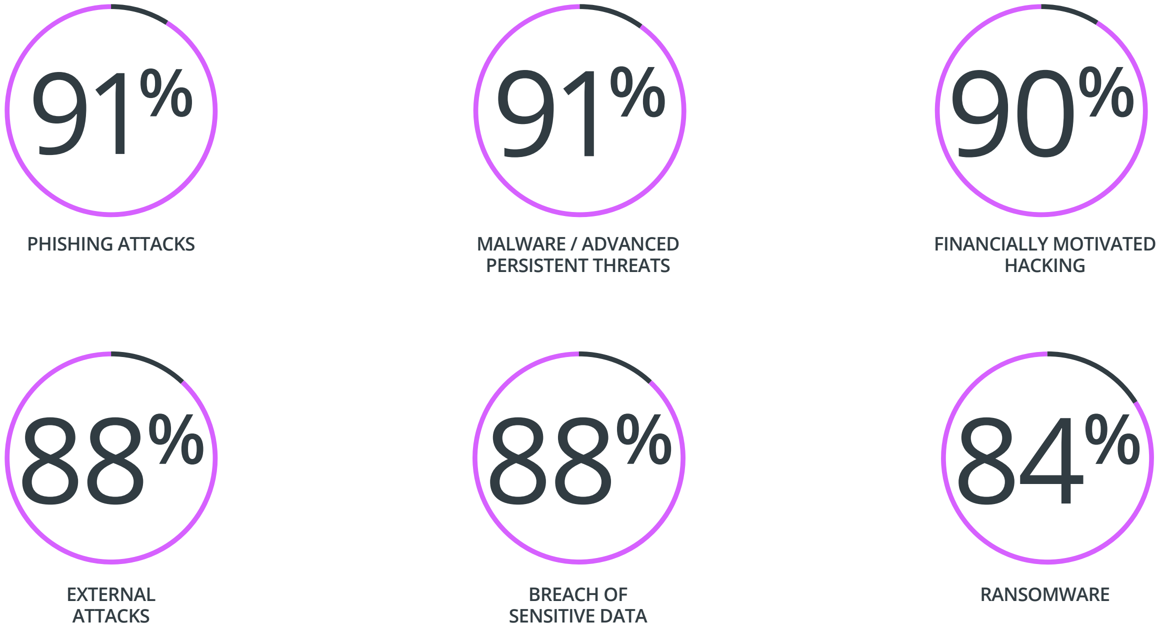
This despite the fact that executives don't think these risks are going away anytime soon. In fact, phishing attacks (91 percent), malware and advanced persistent threats (91 percent), financially-motivated hacking (90 percent), external attacks (88 percent), and data breaches (88 percent) were the top risks expected to increase or stay the same over the next 12 months.

When asked which security risks they feel their organizations are best equipped to handle, 84 percent of security professionals cite data breach of sensitive information. This could be because they've increased investment in data privacy solutions over the the past year as a result of Equifax, GDPR and others. Insider threats came in second place, at 83 percent. Confidence is high for all categories, however. Seventy-five percent or higher are confident that they are equipped to handle each risk surveyed.

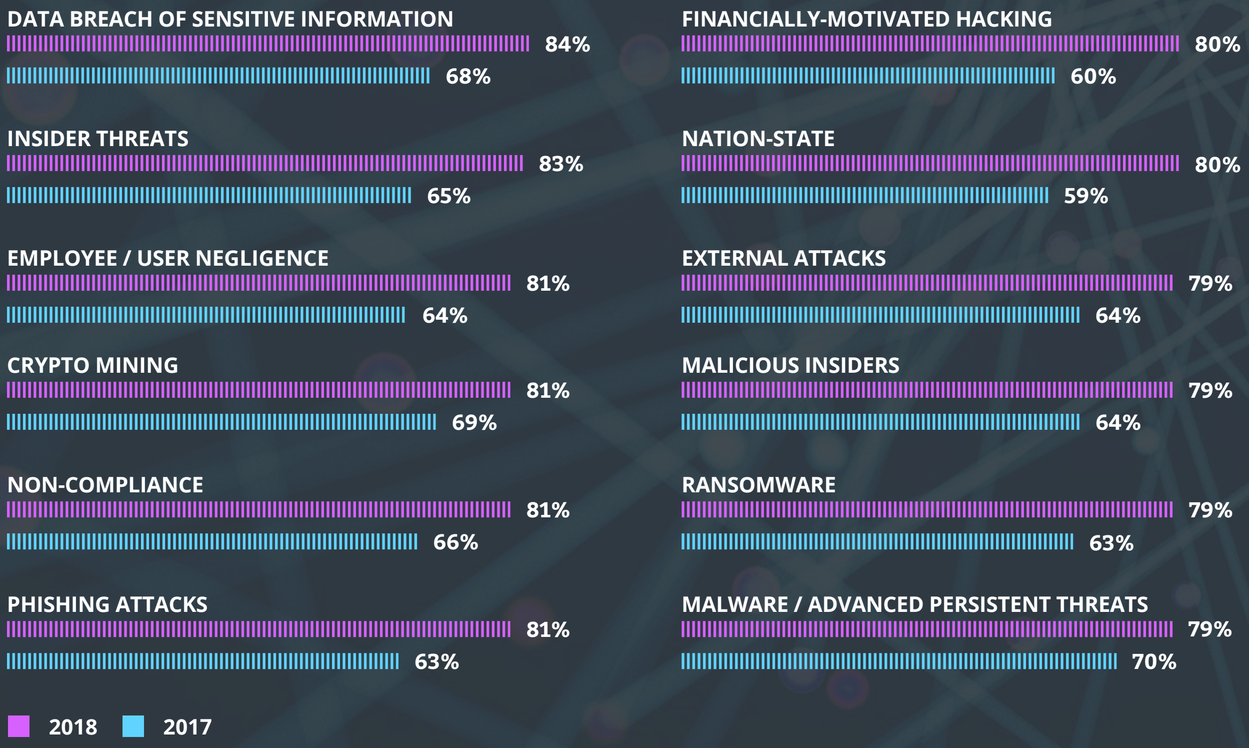


78% OF SECURITY PROFESSIONALS FEEL THEY ARE WELL EQUIPPED TO HANDLE CYBERSECURITY RISKS, A **17% INCREASE FROM 2017**

TOP RISKS EXPECTED TO INCREASE OR STAY THE SAME IN 2019



EXECUTIVES FEEL MORE CONFIDENT THAT THEY ARE EQUIPPED TO HANDLE SECURITY RISKS



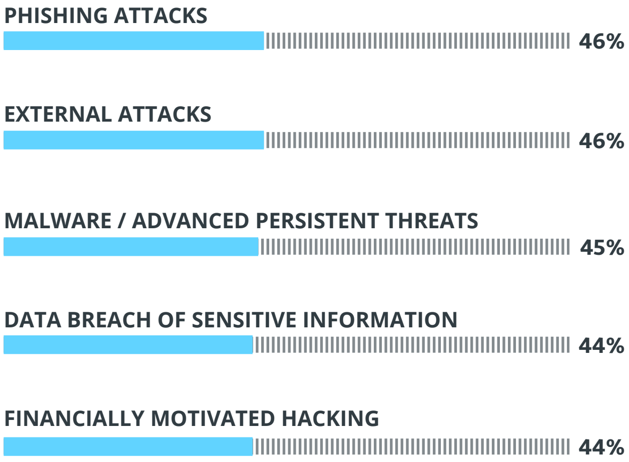
Data Breaches and Hackers Remain Top of Mind

Though confident they have the right controls in place, executives continue to worry about data breaches. Malware and advanced persistent threats are a fast growing concern as nation-state attacks continue to make headlines.

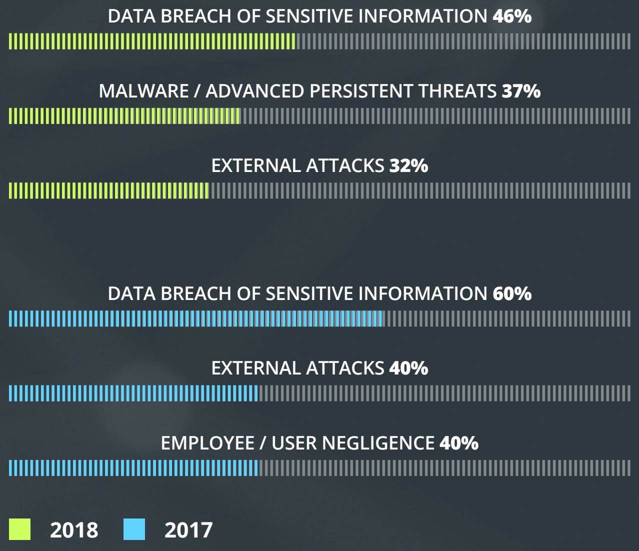
As the threat landscape grows more complex, concerns have spread across multiple risks, but data breaches continue to remain top of mind for executives. When asked to list their top three IT security risks, nearly 46 percent cite data breach of sensitive information, though this is a 16 percent decline from 2017. This was followed by malware and advanced persistent threats at 37 percent and external attacks at 32 percent. When asked what keeps them up at night with regard to protecting data, almost half say hackers, the same top concern as last year. Forty-six percent think phishing and external attacks will increase over the next 12 months.

In terms of top issues keeping people up at night, lack of data privacy controls went down from 46 percent in 2017 to 28 percent in 2018. This indicates that executives feel they have a handle on data privacy, likely due to increased investment in new data privacy controls as a result of incidents like Cambridge Analytica and regulations like GDPR.

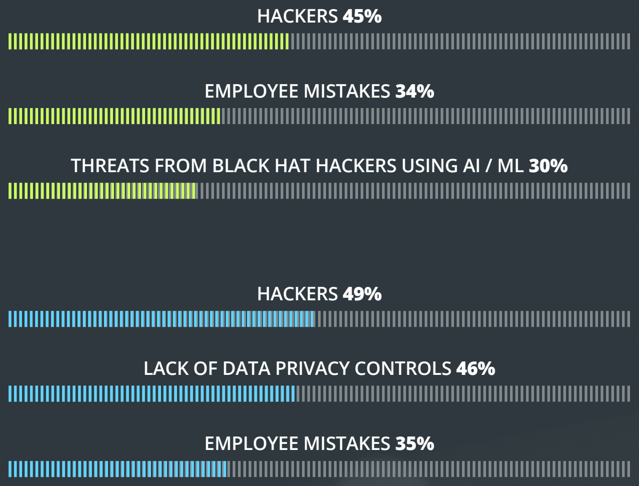
TOP SECURITY RISKS EXPECTED TO INCREASE IN 2019



TOP THREE IT RISKS ACROSS ORGANIZATIONS



TOP THREE ISSUES KEEPING PROFESSIONALS UP AT NIGHT



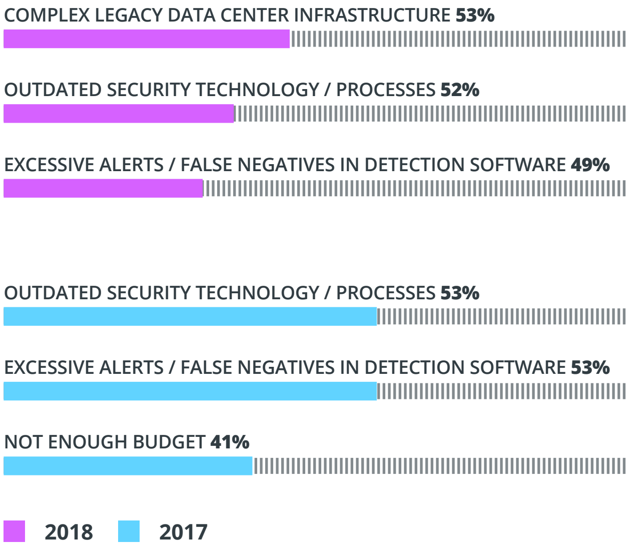
Shortcomings of Legacy Tech Hold Businesses Back

Security technology is in need of an update, though budget constraints are no longer a main obstacle for businesses.

With increasing confidence—and increased investment—in security controls, what's keeping organizations from realizing their full potential? Legacy data center infrastructure clinched the top spot in 2018 for obstacles executives feel are holding their organization back from achieving the security posture it needs (53 percent). This remains constant from 2017, suggesting a need for organizations to invest in more modern solutions that better address their needs.

Outdated security technology and processes (52 percent) and too many alerts (49 percent) continue to plague businesses, while lack of budget has fallen off the list of top obstacles, decreasing from 41 percent in 2017 to 30 percent in 2018.

TOP THREE OBSTACLES TO ACHIEVING SECURITY POSTURES



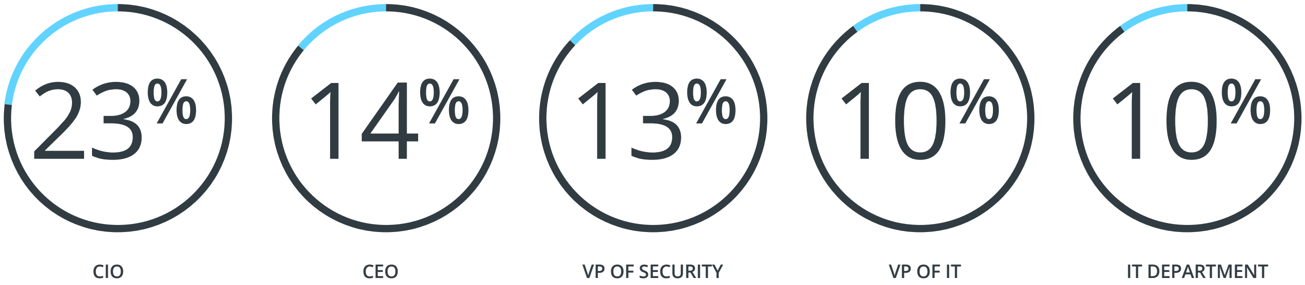
Accountability Rises to the C-Suite

Cybersecurity is now elevated to the highest levels of management.

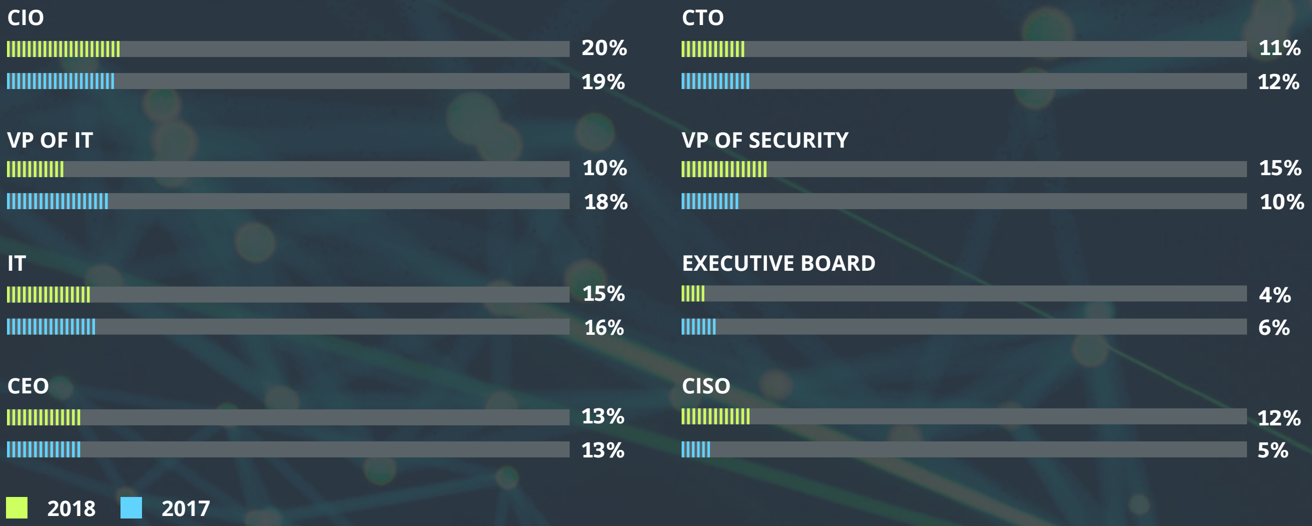
Fifty-eight percent of executives say a member of the C-Suite is ultimately accountable for the security of their organization. Of the C-suite, CIOs took the lead at 20 percent.

When asked who has ultimate responsibility for data privacy efforts specifically, executives remained consistent in their responses: 23 percent say the CIO is responsible for data privacy. The CEO, however, takes second place in responsibility for these efforts, at 14 percent.

RESPONSIBILITY FOR DATA PRIVACY REMAINS WITH MANAGEMENT



ULTIMATE SECURITY ACCOUNTABILITY RESTS WITH EXECUTIVES



Conclusion

Data breaches and data privacy regulations over the past year have begun to influence incremental action by security leaders. They've become a forcing function for increased investment in data privacy solutions and have fostered a new approach to security as a holistic part of the organization.

Despite the fact that the threat landscape remains complex—and they agree it's not going to get any better—executives are more confident than ever that they are well equipped to handle risk. This indicates that investments in technology and personnel in 2017 and 2018 have left security professionals feeling prepared to mitigate risk despite their awareness of the need to adapt and evolve with the ever changing threat landscape.

The fact that increased spending is correlated to greater confidence is an important signal that new solutions are delivering a strong return on investment. As threats and risks continue to rise, we expect executives will continue to turn to security software spending with confidence that it can address their needs.

Methodology

Scale Venture Partners surveyed a representative sample of security leaders in the United States who are responsible for security buying decisions, the success of security deployments, or the overall security of the company. This survey was conducted in December 2018 and reflects sentiments and priorities for 2018 and into 2019. For all questions and responses concerning current risks and priorities, the year referenced is 2018.

PERCENTAGES ON THE FOLLOWING PAGES ADD UP TO 300 PERCENT (NOT 100 PERCENT) BECAUSE RESPONDENTS WERE ASKED TO SELECT THEIR TOP THREE CHOICES:

- Top Technology Investments in 2019 (page 5)
- Confidence Skyrockets Despite Continuance of Threats (page 7)
- Data Breaches and Hackers Remain Top of Mind (page 9)
- Top Three Obstacles to Achieving Security Postures (page 10)

The web-based survey was fielded December 6, 2018 through December 11, 2018 with a sample size of 303 individuals. The margin of error for the survey was 5.6%.