Cybersecurity Perspectives 2020

Security and Privacy in the New Regulatory Era

Table of Contents

Introduction

With each passing year, security grows more complex as hackers find new ways to threaten organizations and businesses race to keep up with new and evolving security solutions. 2019 was no exception. Investor interest in the space led to mega funding rounds for OneLogin, Cloudflare, and BlueVoyant, while Crowdstrike entered the public markets with a bang, demonstrating the voracious appetite for solutions that mitigate security risk. This appetite was fueled by high-profile breaches like those of Capital One, Facebook, and Moviepass that reinforced consumers' concerns that their data isn't safe.

> **A single breach costs an organization nearly $4 million on average[1] and analysts project the total cost of all cybercrime to reach $1 trillion in 2019.[2]**

On top of these threats, businesses have to deal with emerging regulations like EU's General Data Protection Regulation (GDPR) and the brand new California Consumer Privacy Act (CCPA), which came hot on GDPR's heels, allowing no down time for businesses. Current and future regulations are forcing companies to rethink how they protect consumer data.

> **Companies are scrambling to ensure they're compliant in order to avoid penalties, but also to avoid incidents that could damage their brand and lose them customers.**

With security risks rising and regulations looming, how are business leaders feeling? Our survey found that executives are confident they can address the increasingly complex compliance requirements and the growing risks facing their organizations.

> **This indicates that the steps businesses have taken to mitigate risk, such as investing in security software, building in-house solutions, and integrating security throughout their organizations, are successfully addressing executives' concerns, despite an ever-growing attack surface.**

[1] *https://www.ibm.com/security/data-breach.*

[2] *https://www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html.*

Key Findings

Privacy regulations prompt change. GDPR and CCPA have altered approaches to data privacy. Ninety-six percent of respondents have changed their strategy around data privacy compliance.

Organizations continue investing in both on-prem and cloud security solutions. Over two-thirds of respondents are investing in both data center or server security (68 percent) and cloud application security (67 percent). A majority of security executives are planning to invest more in cloud infrastructure security (62 percent) and cloud application security (58 percent) in the next 12 months.

Executives remain confident that their organizations are equipped to manage security risks. Seventy-three percent of executives feel equipped to handle risk, a slight decrease from 2018 (78 percent) but a 12 percent increase from 2017. Eighty-seven percent of executives feel they are at least somewhat more equipped than they were a year ago to handle risks.

Despite confidence, hackers remain top of mind for businesses. The top issues keeping executives up at night are threats from hackers using machine learning to attack businesses and hackers generally. Security issues related to migration to the cloud ecosystem follows closely behind, reflecting the complexity and nascency inherent in hybrid cloud environments.

Legacy technology continues to be an obstacle. For the second year in a row, respondents see complex legacy data center infrastructure (50 percent), outdated security technology and processes (44 percent), and too many alerts or false negatives with detection software (44 percent) as the top obstacles holding their organization back from achieving the security posture it needs. This has forced 65 percent of executives to build security solutions in-house, a 15 percent increase from 2018.

Accountability remains in the C-suite. Sixty-five percent of executives say a member of the C-suite is ultimately responsible for the security of their organization, a 7 percent increase from 2018. For the first time, CEOs topped the list of executives with primary responsibility.

Businesses Adjusting to New Data Privacy Challenges

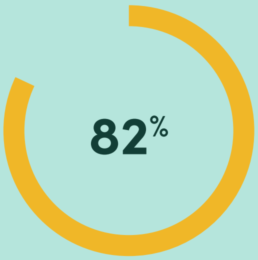
GDPR and new regulations like CCPA are forcing organizations to rethink business strategies.

GDPR has now been in effect for nearly two years, and the CCPA— which affects any business that collects consumer data from California residents — took effect on January 1, 2020, with enforcement beginning July 1, 2020. As businesses strive to ensure they're remaining GDPR compliant and rush to comply with CCPA before enforcement begins, they're rethinking how they handle consumer data.

Businesses are taking action to avoid exposure to compliance risks. **Ninety-seven percent of executives say their organization has made changes in response to GDPR and CCPA.** Fifty-five percent of organizations have increased metrics and reporting around data privacy compliance, 53 percent have increased investment in new data privacy solutions, and 50 percent have increased training for non privacy-focused personnel over the past 12 months.

These changes are boosting the confidence levels of executives. **Seventy-five percent feel their company is equipped to handle data privacy compliance,** and 82 percent feel their company is at least somewhat more equipped to handle data privacy compliance compared to 12 months ago.

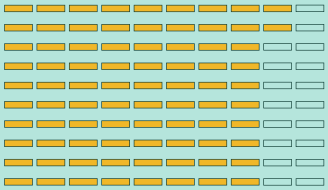
Despite the fact that GDPR fines[3] can go up to $22 million or as high as 4% of global turnover (revenue) and CCPA fines[4] can reach $7,500 per consumer violation, it seems executives don't think they'll be caught in the crosshairs. **Fewer than half of executives (46 percent) are worried about getting fined for privacy regulations under GDPR and CCPA.**



of businesses collect personal information on customers

3/4

of professionals feel their company is equipped to handle data privacy compliance



82%

say their company is at least somewhat more equipped to handle data privacy compliance than 12 months prior

78%

of companies claim they are GDPR compliant

[3] https://www.gdpreu.org/compliance/fines-and-penalties
[4] https://securityboulevard.com/2019/08/what-is-the-ccpa-and-who-must-comply-the-california-consumer-privacy-act-explained

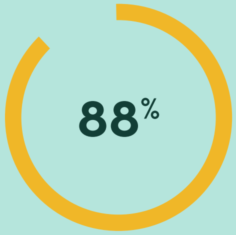
Sixty-five percent of executives think GDPR is effective at protecting consumer privacy — and industry stats would bear that out. Cisco's Data Privacy Benchmark Study[5] found that GDPR-ready companies were less likely to have experienced a breach in the last year. When a breach occurred, fewer data records were impacted and system downtime was shorter, the report found. Because of this, **only 37 percent of GDPR-ready companies had a loss of more than $500,000 last year, versus 64 percent of the least GDPR-ready.**

Executives are conflicted about the need for regulation at the federal level. While just 36 percent think that GDPR provides adequate guidance and enforcement to ensure that businesses properly address data privacy issues in the U.S, **only 24 percent feel there is a need for a federal data privacy regulation.**

When it comes to CCPA and other upcoming regulations, executives are still coming to terms with how to best handle compliance. Asked about the biggest regulatory compliance hurdles their organizations face, executives cite **the need to understand which data is being collected on consumers (37 percent) and the need to devise an easy way to comply with consumer requests (35 percent)**. When it comes to compliance, executives are most concerned that their brand will be damaged (45 percent) or that they will lose customers (35 percent) if they are found to be non-compliant, and that compliance will be costly (35 percent).

84%

are taking steps to be CCPA compliant



think they will be CCPA compliant by the time enforcement starts on July 1, 2020

46%

are worried about getting fined for privacy violations under GDPR or CCPA

Over the past year, how has your organization adapted in response to the GDPR compliance deadline (May 2018) or the California Consumer Privacy Act (CCPA)?[6]

55%

Increased measurement and reporting around data privacy compliance

53%

Increased investment in new data privacy solutions

50%

Increased training for non privacy focused personnel

48%

Increased investment in data privacy personnel

44%

The CEO and/or board is more involved in decisions around data privacy

3%

No changes made

[5] *https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf*

[6] *Percentages in this graph do not add up to 100 percent because respondents were asked to select all that apply.*

Over the past year, how have you changed your processes / strategy around data privacy compliance?

52%

Increased integration of data privacy with other teams, e.g. IT, operations and software engineering

50%

Increased metrics and reporting around data collection and compliance

48%

Provided greater visibility and transparency into the state of data privacy within the organization

46%

Applied stricter enforcement of data privacy policies

43%

Expanded accountability for data privacy across the business

35%

Hired more data privacy compliance personnel

27%

Reduced the amount of customer data we collect, share or sell

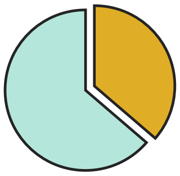
24%

Hired a Chief Privacy Officer

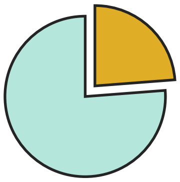
4%

We have not changed our processes or strategy around data privacy

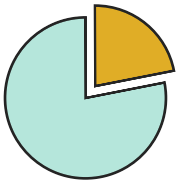
What is your point of view around data privacy regulations in the US?



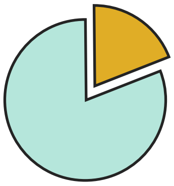
36%
GDPR provides adequate guidance and enforcement to ensure that businesses properly address data privacy issues in the U.S.



24%
There is a need for a federal data privacy regulation in the U.S.

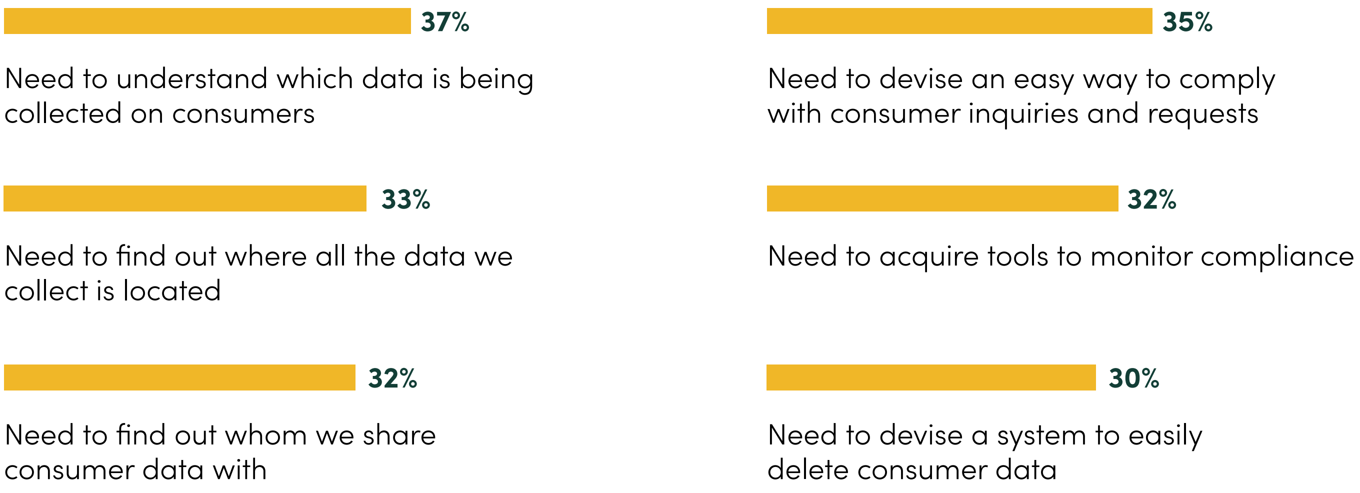


22%
Data privacy is best handled by individual organizations



19%
GDPR does not provide adequate guidance and enforcement to ensure that businesses properly address data privacy issues, but state-specific data privacy regulations, such as CCPA, are adequate to do so

What are the biggest hurdles your organization will have to overcome to become compliant with CCPA and other data privacy regulations?[7]



What are the biggest concerns about having to be compliant with CCPA and other data privacy regulations?[8]

45%

Our brand or reputation will be damaged if we are found not to be in compliance, or if we are forced to disclose breaches

35%

We will lose customers if we are found not to be in compliance, or if we are forced to disclose breaches

35%

Compliance will be costly

30%

It will negatively impact sales and marketing effectiveness, decreasing new business bookings

30%

If consumers demand that we stop selling data, our revenue will be adversely impacted because we monetize consumer data

26%

If we fail to comply, we will be fined

[7] Percentages in this graph do not add up to 100 percent because respondents were asked to rank in descending order.

[8] Percentages in this graph do not add up to 100 percent because respondents were asked to rank in descending order.

Organizations Adopt a Two-Pronged Approach to Security

Organizations are increasingly investing in both on-prem and cloud security solutions.

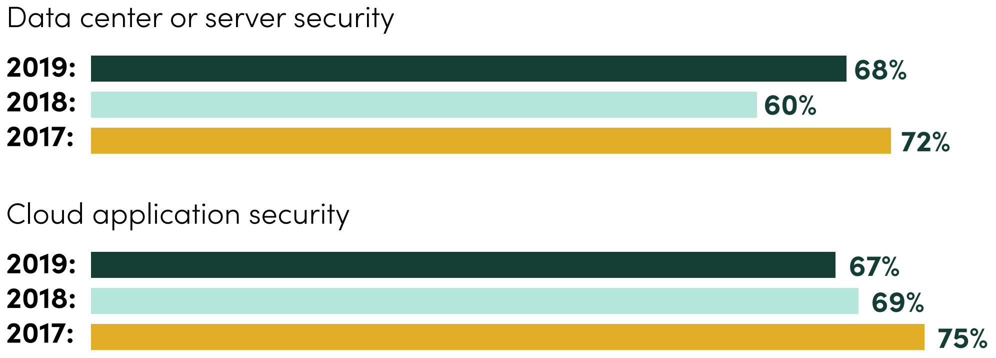
Data center spending is rising and with it the need for security for all that data stored there. **Sixty-eight percent of executives cite data center or server security as a top investment priority,** a small increase in number (60 percent), but a big leap from fifth place in 2018.

Along with data center security, executives continue to prioritize cloud security. **Over two thirds of executives are investing in cloud application security (67 percent)** and over half plan to invest in cloud infrastructure security (62 percent) and cloud application security (58 percent) over the next 12 months.

Businesses are continuing to approach security holistically. **Sixty-seven percent of executives have increased integration of security with other teams in their organization, and 57 percent have increased metrics and reporting around security.** When it comes to IT security strategy, executives are looking at which threats and vulnerabilities need to be attended to (26 percent), as well as regulatory measures around data privacy and security (22 percent).

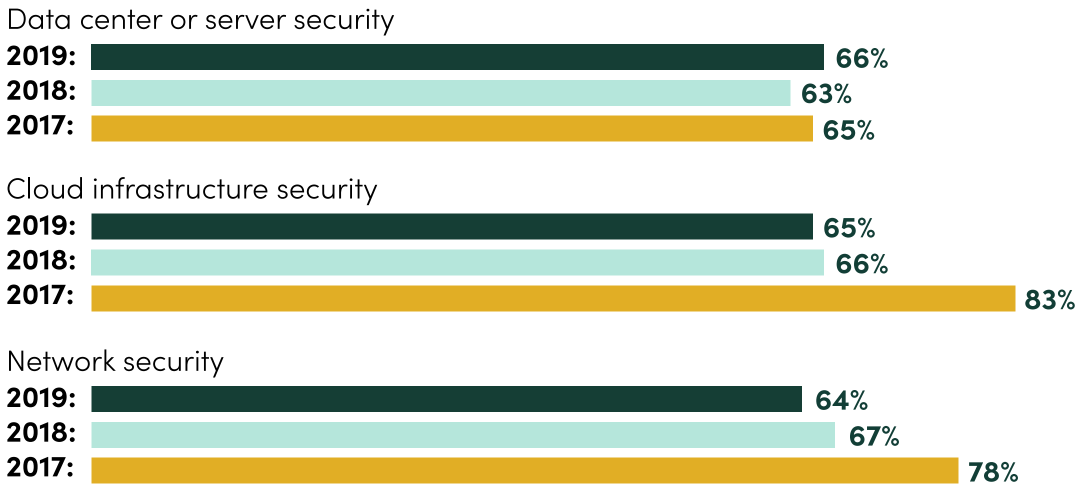
Recent geopolitical shifts, including trade wars, Brexit and market volatility, have also prompted organizations to adjust their security strategies. **Sixty percent have increased their investment in security solutions as a result of these global trends and geopolitics, and 57 percent have placed a greater emphasis on security and compliance policy management.** Fifty-seven percent are more concerned about their ability to protect their company from cybersecurity attacks in light of the upcoming U.S. 2020 election.

Top technology investments in 2019:[9]

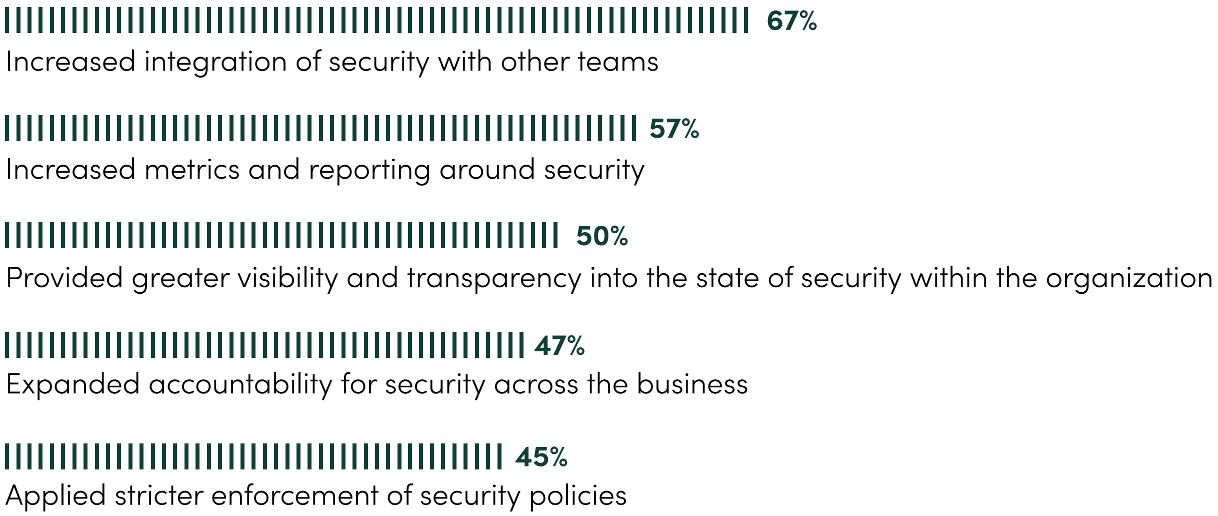

Data center or server security

Cloud application security

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



Over the past year, how have you changed your processes or strategy around security?



Top drivers for IT security strategy:

26%

Decide based on threats and vulnerabilities that need to be attended to

22%

Decide based on regulatory measures around data privacy and security

16%

Decide based on changes to the company's business strategy

15%

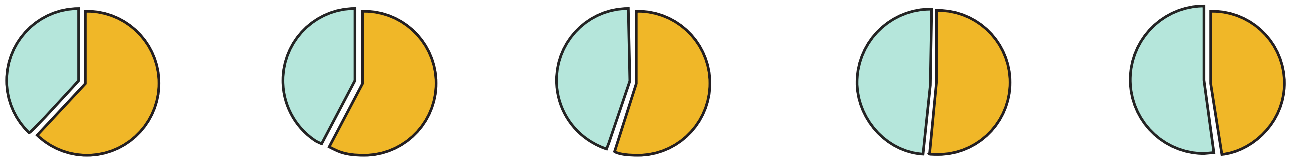
Use a risk-based approach

9%

Decide based on which parts of the program need to mature or evolve

2020 Projections:

Top technology investment priorities projected for 2020:



62%
Cloud infrastructure security

58%
Cloud application security

55%
Network security

52%
Data security or data loss prevention

48%
Data privacy

Which of the changes below have you made to your security strategy in the past 12 months due to recent geopolitical shifts, including trade wars, Brexit, and market volatility?[10]

60%
Increased investment in security solutions

57%
Placed greater emphasis on security and compliance policy management

52%
Increased investment in security personnel

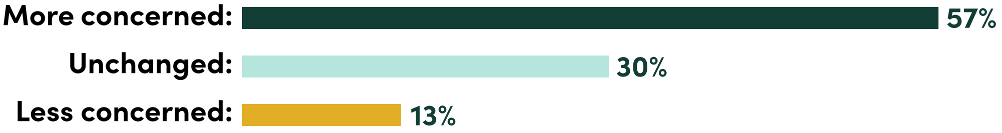
42%
Placed greater emphasis on addressing nation-state attacks

34%
Switched vendors for specific security technologies

5%
Made no changes

How the upcoming U.S. 2020 election impacts executives' ability to protect their business

Level of concern about their ability to protect their company from cybersecurity attacks



[10] *Percentages in this graph do not add up to 100 percent because respondents were asked to select all that apply.*

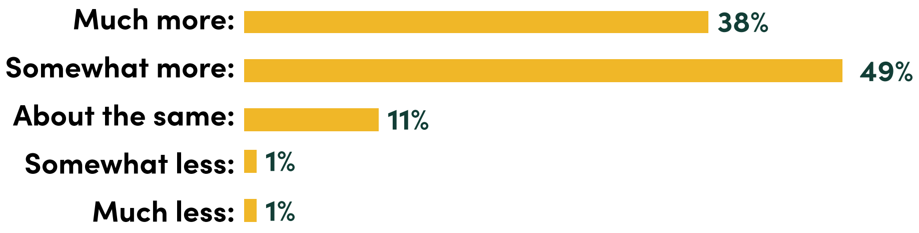
Confidence Remains High Amidst Continued Threats

Despite an ever-evolving threat landscape, executives remain confident that they're equipped to effectively manage risk.

There is a contradiction in executive sentiment related to security threats. While executives realize the severity of the risks they face, they also feel optimistic that they will be able to counter those threats. **Despite an active threat environment, 73 percent of professionals feel they are well equipped to handle cybersecurity risk,** which is consistent with 2018 (78 percent). Eight-seven percent feel they are at least somewhat more equipped to handle risk than a year ago.

That confidence may be at least partly due to the fact that they are investing more in security overall. **Security spending is expected to reach $133.8 billion by 2022,[11] giving security teams more tools and firepower at their disposal to manage threats and mitigate risk.** The three security threats they feel most equipped to handle are: malware and advanced persistent threats (83 percent), financially motivated hacking (82 percent), and non-compliance (82 percent).

Compared to 12 months ago, is your company NOW more or less equipped to handle cybersecurity risks?



73%

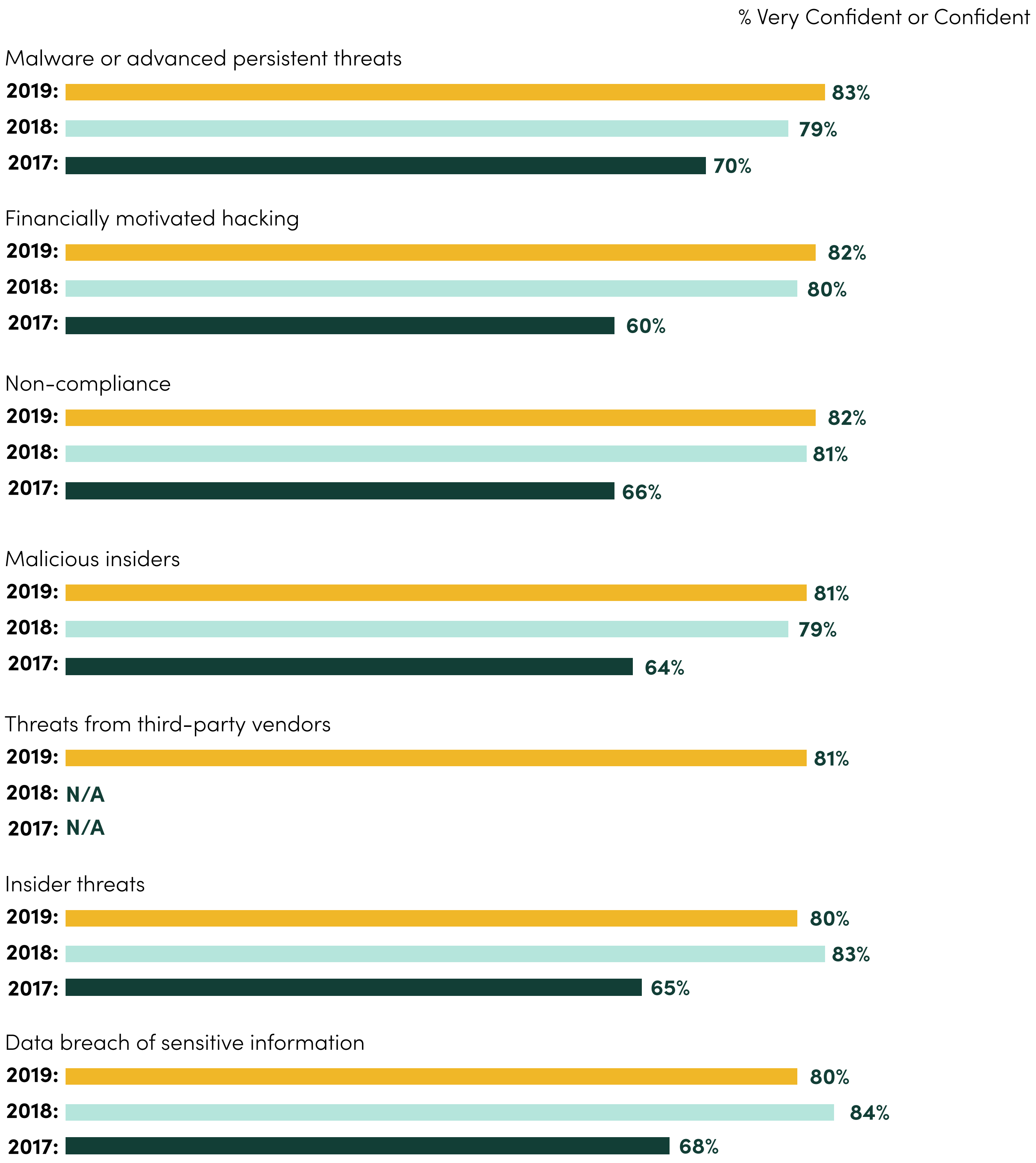
of security professionals feel they are well equipped to handle cybersecurity risk.

Top risks expected to increase or stay the same over the next 12 months:

- Phishing attacks
- Financially motivated hacking
- Malware or advanced persistent threats
- Ransomware
- Data breach of sensitive information
- Nation-state

[11] https://www.idc.com/getdoc.jsp?containerId=prUS44935119

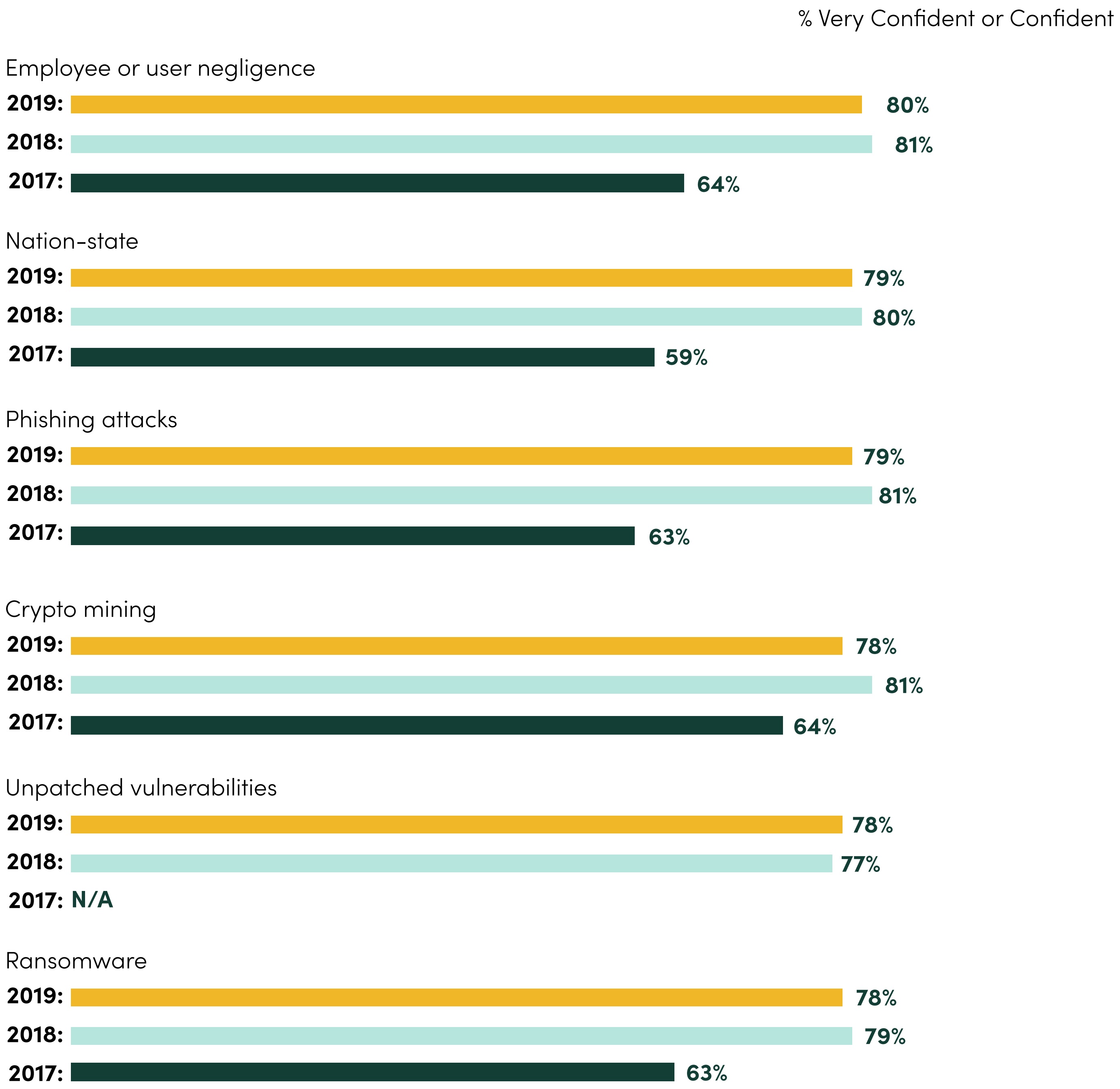
For each IT security risk, please rate your level of confidence that the current controls your company has in place are effectively managing the risk.



10. Percentages in this graph do not add up to 100 percent because respondents were asked to select all that apply.

11. https://www.idc.com/getdoc.jsp?containerId=prUS44935119

For each IT security risk, please rate your level of confidence that the current controls your company has in place are effectively managing the risk.



Breaches Remain Top of Mind as Regulation Ramps Up

The intensifying regulatory environment is prompting executives to think about the consequences of a breach.[12]

Against a backdrop of more and more breaches — in the first nine months of 2019, 5,193 breaches exposed 7.9 billion records[13] — regulation is rising. Many companies are still struggling to meet the requirements of GDPR and now they're facing strict CCPA guidelines too. Meanwhile, more regulations are being proposed at both the state and federal levels as the **industry and lawmakers try to figure out how to best deal with a patchwork of state laws and debate whether to adopt a nationwide regulation.**

It's no surprise that breaches and compliance are key concerns now for security executives. **Forty-six percent cite data breach of sensitive information as a top three IT security risk.** This is followed by malware or advanced persistent threats (36 percent), which is consistent with 2018. For the first time, phishing attacks entered the list of top three risks, at 31 percent. This could be because phishing accounted for 21 percent of breaches in 2019, the second largest cause of breaches reported by U.S. companies.[14]

Executives are not only concerned about breaches, but also about the threat actors behind them. With hacking being the cause of 52% of breaches in 2019,[15] hackers continue to keep executives up at night (26 percent), although this is a 19 percent decline from 2018. **Hackers using AI or ML to attack businesses (26 percent) is a rising concern, from the No. 3 rank in 2018 to tied for No. 1 in 2019, as hackers start to experiment with tactics like AI-powered malware and "smart" phishing.[16]**

Another major concern is threats in the cloud. With the cloud computing market expected to grow to $623.3 billion by 2023,[17] cloud risks are coming to the forefront. This was seen in the 2019 Capital One breach, which resulted from a misconfigured setting on a system that allowed the bank to communicate with Amazon Web Services, the bank's cloud provider.[18] That's likely why **24 percent cite migration to the cloud ecosystem as a top three concern.**

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

[13] https://pages.riskbasedsecurity.com/data-breach-quickview-report-2019-q3-trends

[14] https://www.f5.com/labs/articles/threat-intelligence/2019-phishing-and-fraud-report

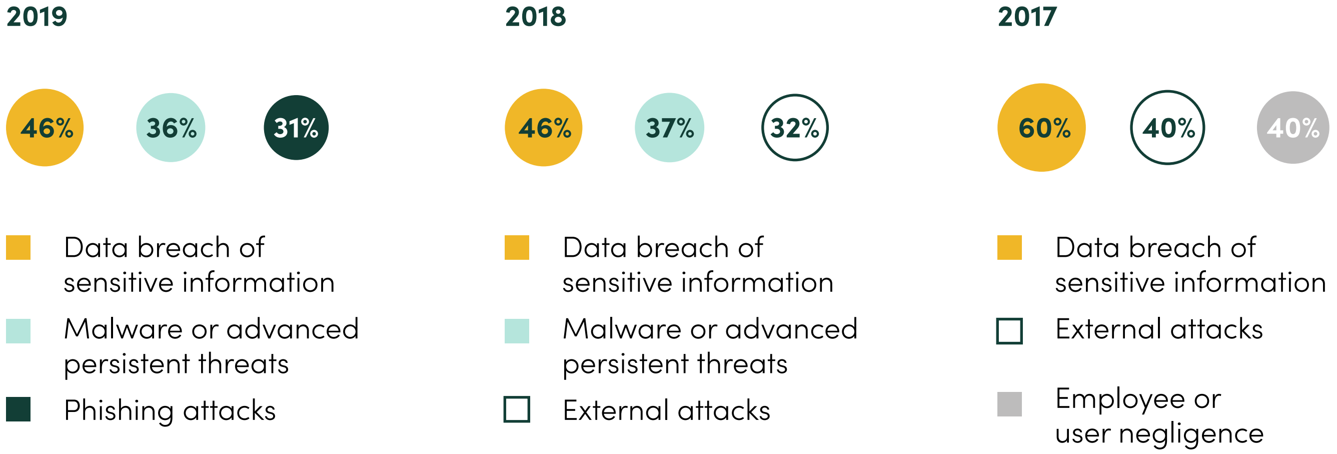
[15] https://www.business.com/articles/small-business-data-breaches

[16] https://www.cpomagazine.com/cyber-security/ai-powered-malware-smart-phishing-and-open-source-attacks-oh-my-the-new-wave-of-hacking-in-2019-and-how-to-prevent

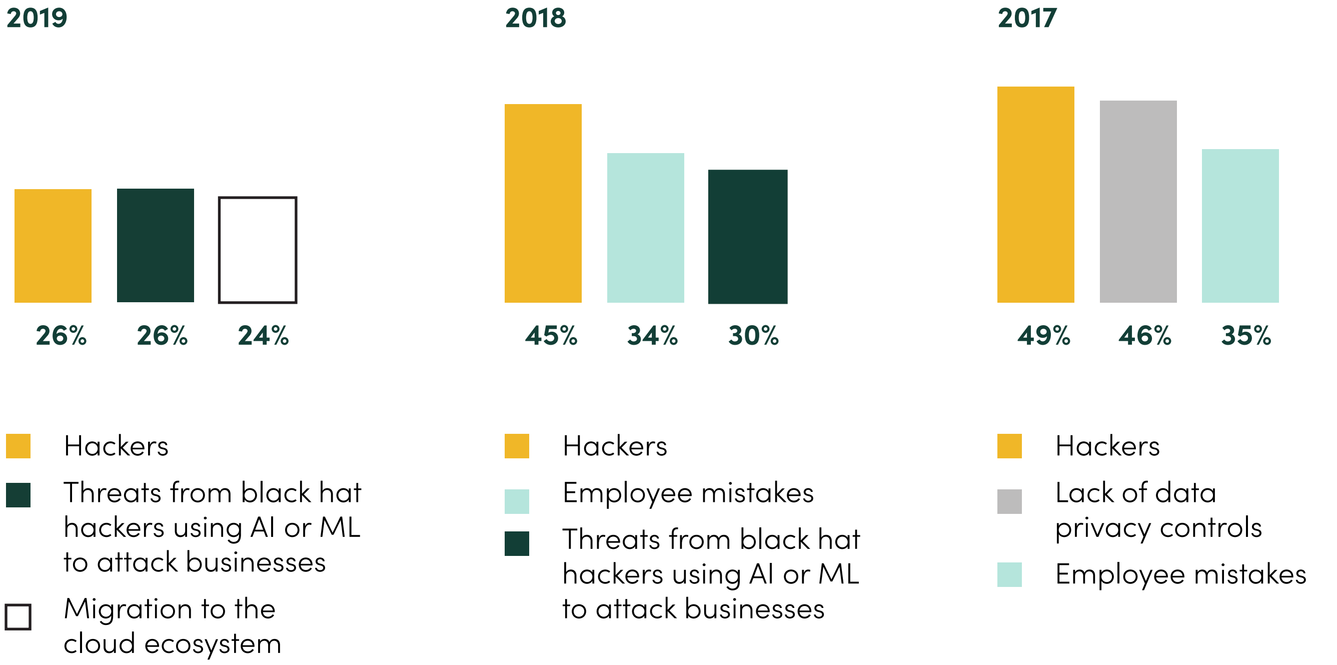
[17] https://www.prnewswire.com/news-releases/cloud-computing-market-worth-623-3-billion-by-2023--exclusive-report-by-marketsandmarkets-300802108.html

[18] https://www.businessinsider.com/capital-one-hack-vulnerability-on-cloud-amazon-known-for-years-2019-8

Organizations' top three IT security risks:



Top three issues keeping professionals up at night with regard to protecting data:



Executives Turn to In-House Security Solutions

Dated security technologies continue to hold businesses back, but executives are struggling to find new commercial solutions that adequately address their needs.

Despite the crowded security vendor space, executives still find they can't just spend more to fix their security problems. For the second year in a row, **complex legacy data infrastructure is the obstacle executives most feel is holding their organization back from achieving the security posture it needs (50 percent)**. Outdated security technology and processes (44 percent) and too many alerts or false negatives with detection software (44 percent) are also listed among the top three obstacles for the third year in a row, which suggests that **businesses are in need of an update but are increasingly failing to find commercial solutions that work for them.**

In fact, the number of executives who have built in-house solutions because they felt there was no viable commercial alternative is rising rapidly. **Sixty-five percent of executives needed to build a security solution in-house over the past 12 months, a 15 percent increase from 2018.** The top areas in which executives built in-house solutions were operational technology (42 percent), data privacy (39 percent), and data security or data loss prevention (38 percent). For security startups wondering which solution to build, look no further than the industries in which organizations are building themselves.

Top three main obstacles holding organizations back from achieving the security postures they need:

2019

1 Complex legacy data center infrastructure **50%**

2 Outdated security tech or processes **44%**

3 Too many alerts or false negatives with detection software **44%**

2018

1 Complex legacy data center infrastructure **53%**

2 Outdated security tech or processes **52%**

3 Too many alerts or false negatives with detection software **49%**

2017

1 Outdated security tech or processes **53%**

2 Too many alerts or false negatives with detection software **53%**

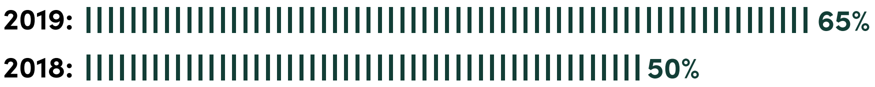
3 Not enough budget **41%**

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

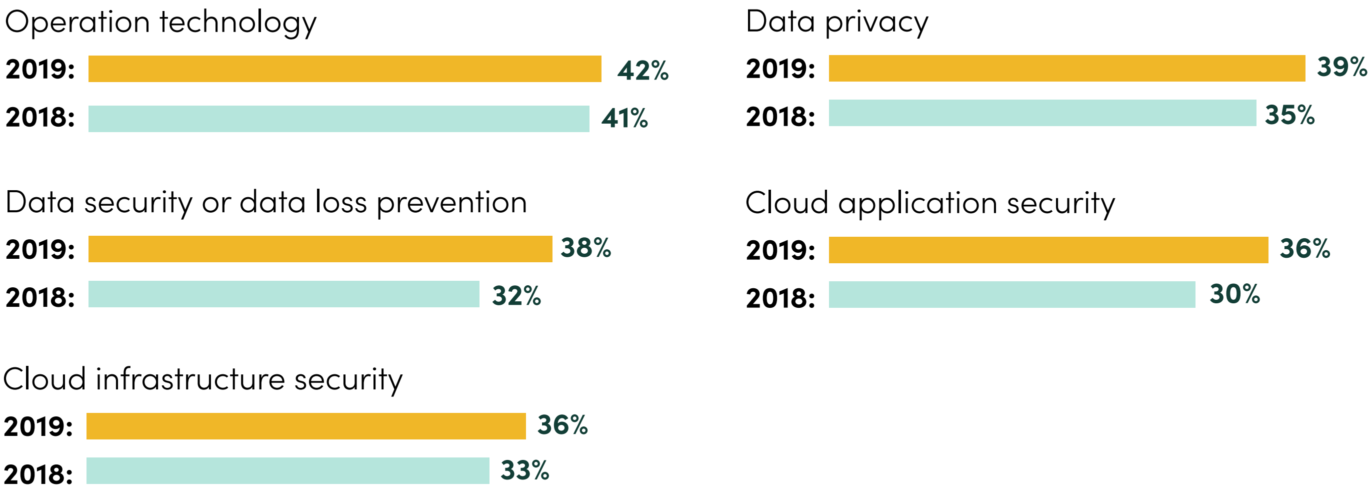
> For the third year in a row, executives ranked "too many alerts or false negatives" as a top obstacle holding their organizations back from achieving the security postures they need. This is clearly a major pain point for CISOs, and one that has arisen because point solutions create extra work for security teams. In today's security environment, the more solutions you invest in, the more personnel you need to hire to monitor them.
>
> Enterprises need to offload this extra work, and a class of startups is cropping up that caters to this need. Savvy security startups realize that enterprises are warming up to security software that comes bundled with services, as long as those services reduce the operational overhead of implementing and maintaining the software. In some ways, the security market is going "back to the future" to the 1980's and 1990's paradigm of software sold alongside services.

Ariel Tseitlin
Partner at Scale

Executives who built in-house in the past 12 months:



Areas in which executives built in-house solutions:



CEOs Seen to Hold Ultimate Responsibility for Their Organizations

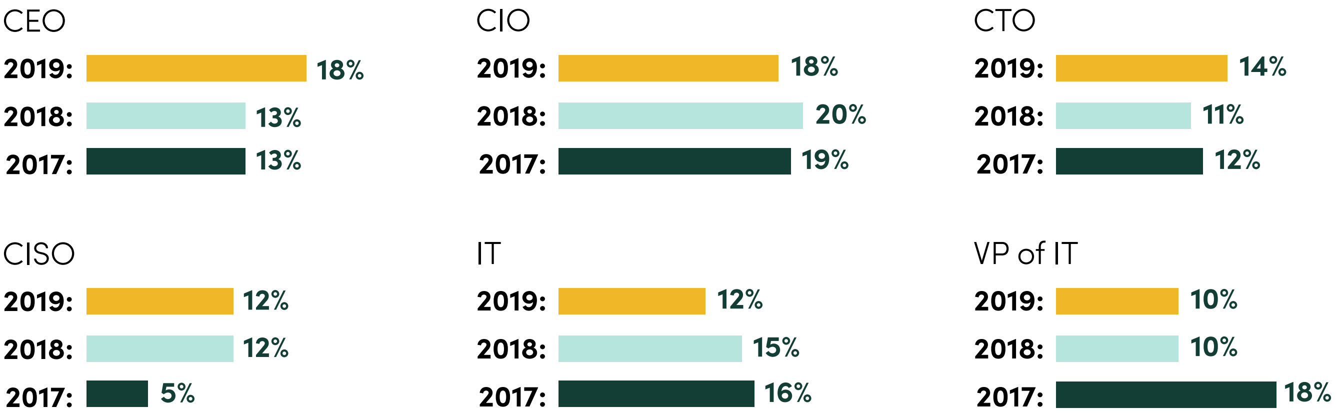
The buck still stops with the C-suite for security and data privacy efforts.

When it comes to who should be held accountable for the security of the organization, business leaders tend to point up the org chart. Asked who holds responsibility for the security of the organization, 65 percent said the C-suite. While most respondents said the CIO should have ultimate responsibility in 2018 (20 percent), this year's respondents said it should be the CEO (18 percent).

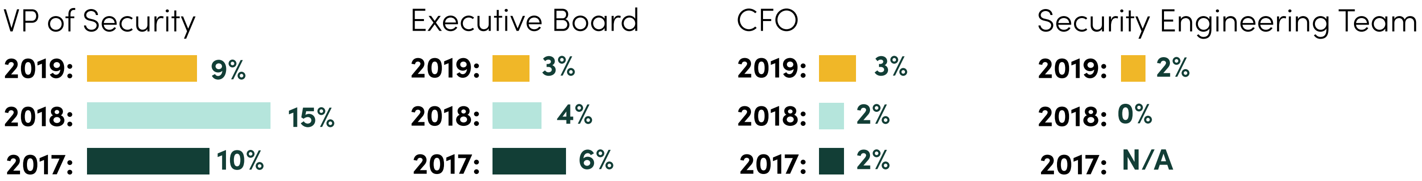
The stats reflect a general view that CEOs are key to the success or failure of security in the organization. For example, a Ponemon study found that 55 percent of executives say a well-informed and involved CEO and board of directors is critical to a strong security posture, and that same percentage said they believe **it's a myth that the CEO and board of directors are too far removed from day-to-day security events to provide effective oversight and compliance.**[20]

Executives feel that upper management should be responsible for data privacy success too. **Sixty-eight percent say the C-suite is ultimately responsible for data privacy efforts.** While responsibility was said to be most shouldered by CIOs in 2018 (23 percent), CEOs took the top accountability spot in 2019, at 19 percent. CTOs are increasingly seen as responsible, up from 9 percent in 2018 to 15 percent in 2019. Only 5 percent said the CPO is ultimately accountable, which shows that most companies have yet to create or hire for this position. Given emerging privacy regulations, we expect more companies to see the need for a dedicated privacy officer at the C-level.

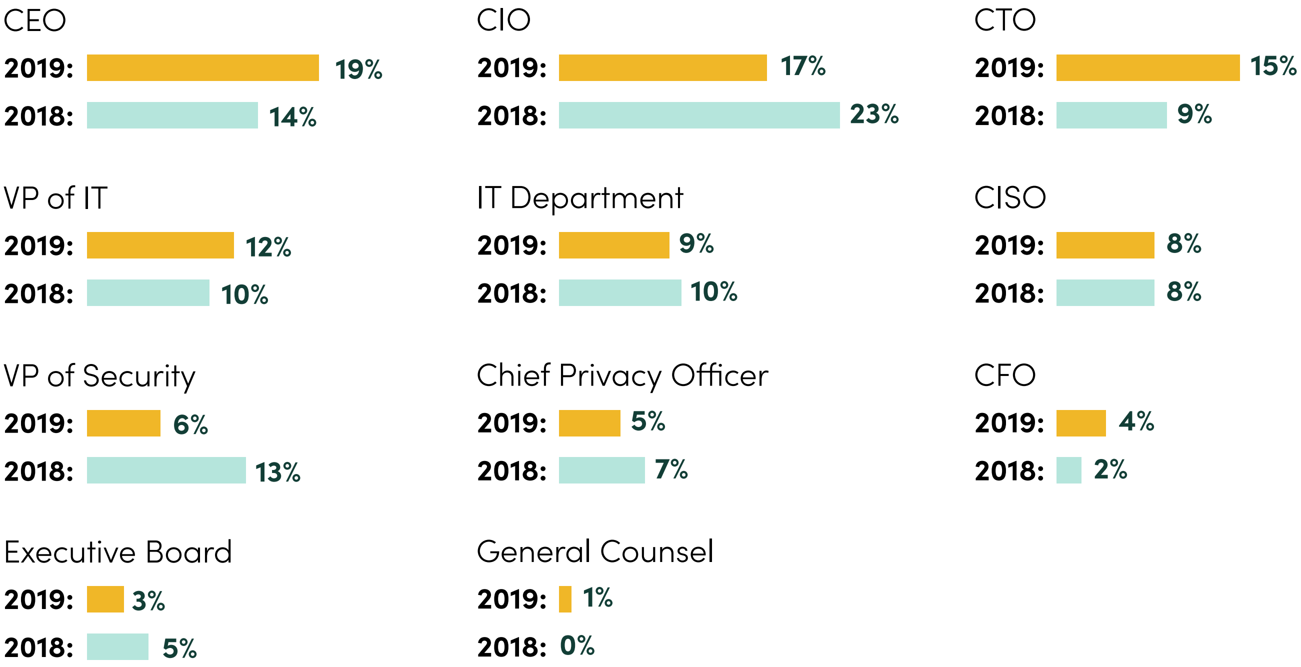
In your organization, who is ultimately accountable for security?



[20] https://www.bmc.com/content/dam/bmc/collateral/third-party/Ponemon%2bReport.pdf



Who has ultimate responsibility for data privacy efforts at your organization?



Conclusion

A new and increasingly complex regulatory environment is taking shape, which will only make it harder for companies to know how to secure and protect their data to meet guidelines.

> **With five states drafting data privacy regulations in addition to California,[22] and dozens more on the horizon, it will become increasingly challenging for companies to reach compliance without prioritizing and following best practices for it.**

The CPO and the General Counsel, among other top executives, will need to spend more time on data privacy issues to ensure that breaches don't disrupt operations, anger customers, and attract the attention of regulators.

Methodology

Scale Venture Partners commissioned Market Cube to conduct a survey of 301 security leaders in the United States who are responsible for buying decisions, the success of security deployments, or the overall security of the company. The web-based survey was fielded December 6 through December 11, 2018 with a sample size of 301 individuals. The margin of error is plus or minus 5.6 percentage points. This survey was conducted in October 2019 and reflects sentiments and priorities for 2019 and into 2020. For all questions and responses concerning current risks and priorities, the year referenced is 2019.