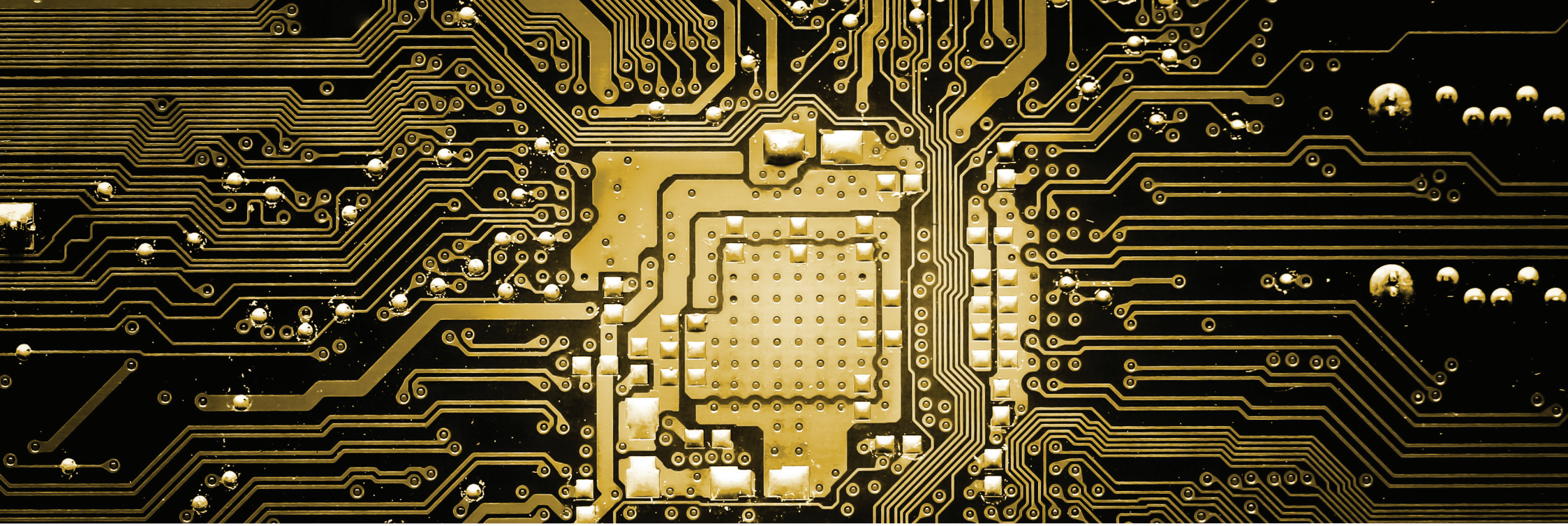


Data Center Survey Reveals Cybersecurity Awareness Gaps

MARIA KOROLOV

Published October 2019

DataCenter Knowledge™

Table of Contents

Executive Summary

Data centers were less vulnerable to cyberattacks last year than they were in 2017, according to the Trends in Data Center Network and IT Security survey, with much of the improvement due to better end-user training and education.

In addition, respondents said they were better able to secure connections to public clouds and had improved internal IT processes such as patching and decommissioned legacy hardware. However, the survey also demonstrated some areas where improvement is needed. Data centers still depend too much on traditional passwords instead of adopting multi-factor authentication, behavioral analytics, and other, more modern technologies.

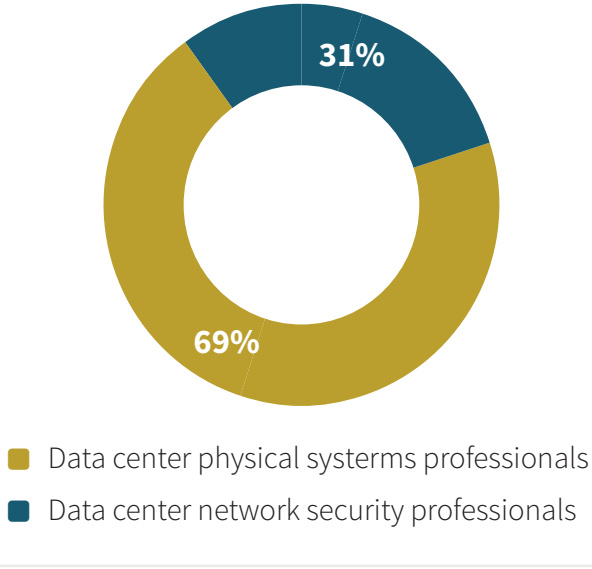
Survey Methodology and Demographics

The survey was conducted online in the summer of 2018 among 477 respondents, including data center professionals with IT or data center network security backgrounds, as well as non-data center IT professionals. Of the data center respondents, 48 percent said IT or data center network security was one of their areas of responsibility, and another 37 percent said they were peripherally involved in cybersecurity.

The respondents came from a wide variety of industries, including data processing and IT services, construction, consulting, education, finance, retail, telecom, healthcare, manufacturing, and government.

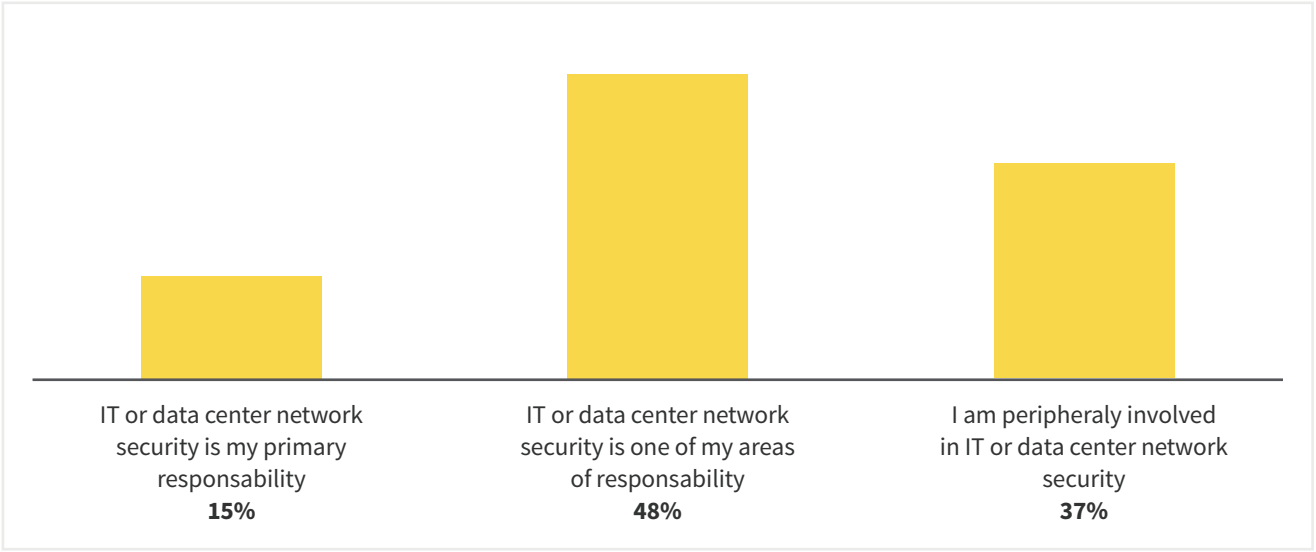
Many different job titles and functions were also represented, including IT staff, IT architect, data center manager, CIO or CTO, database administrator and networking or systems manager. More than a third of respondents had management roles.

Data Center Role



QUESTION: **Which best describes you?**

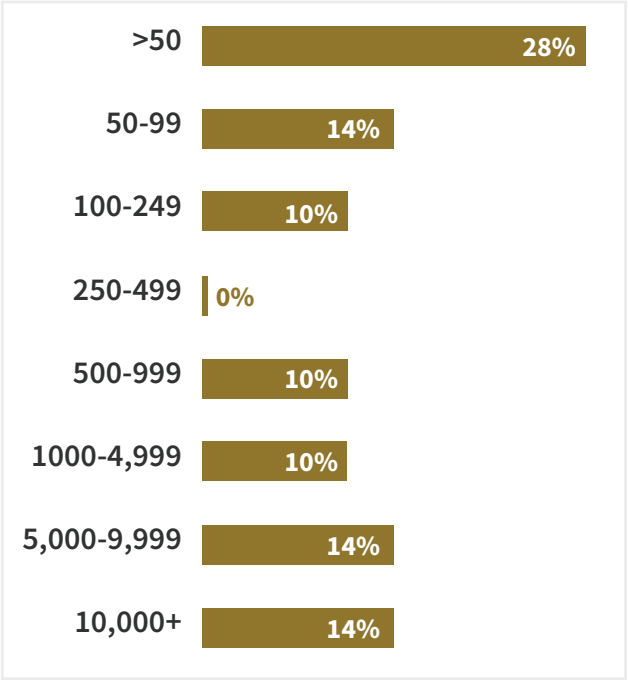
Level of Data Center Network Security Involvement



QUESTION: **Which of the following BEST characterizes yuor involvement in IT or data center network security for you organization?**

Enterprises with 1,000 employees or more accounted for 38 percent of the organizations represented, and 28 percent were from very small companies, with fewer than fifty employees. The rest were mid-sized firms with fifty to a thousand employees.

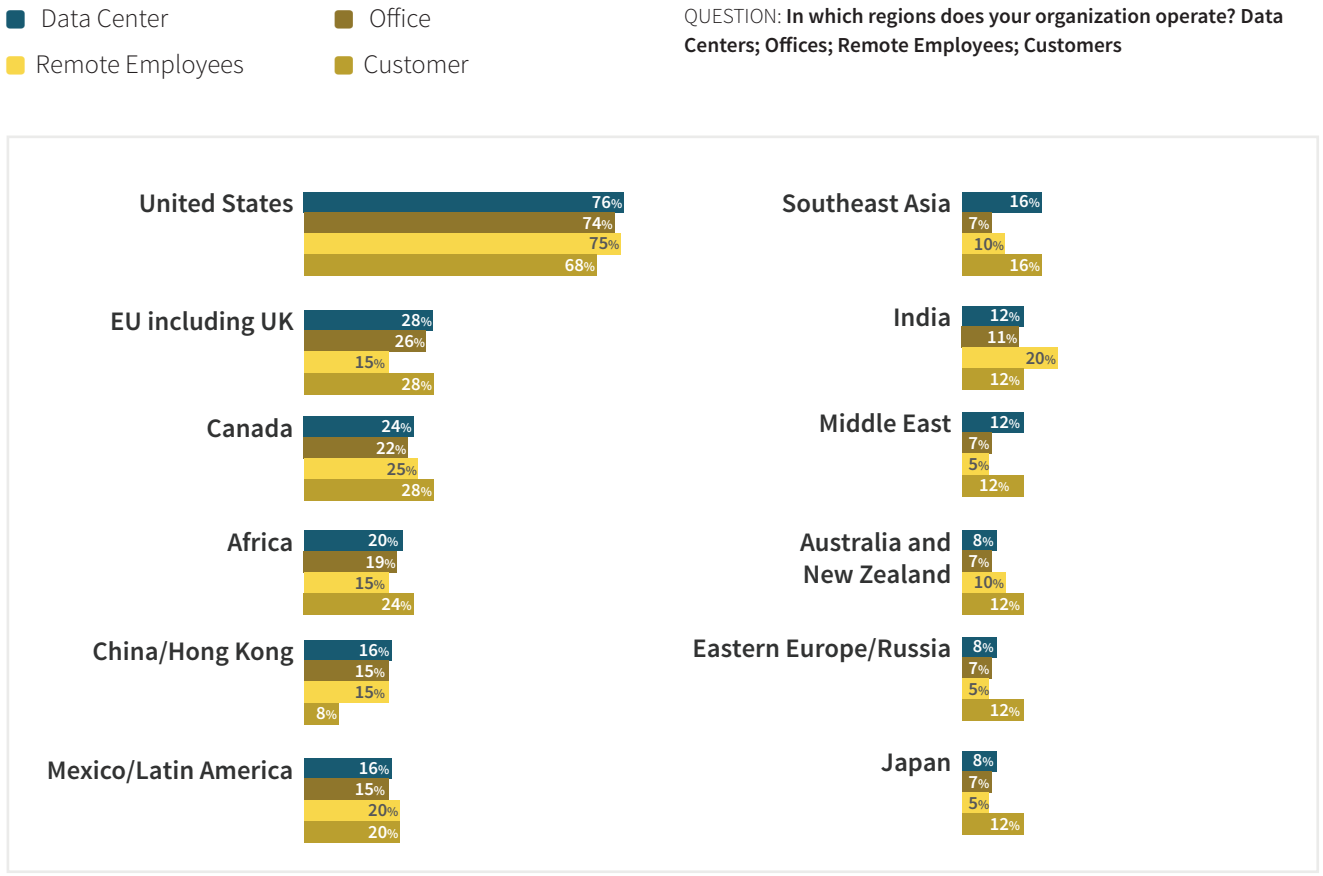
Number of Employees



QUESTION: **How many people are employed by your entire organization (at all locations)?**

Respondent organizations operated primarily in the US, with 78 percent reporting that they had US-based data centers. In addition, 28 percent had data centers in the EU and 24 percent in Canada. Respondents also reported data centers in other locations, including Asia, Africa, and Latin America.

Locations: Data Centers, Offices, Remote Employees & Customers



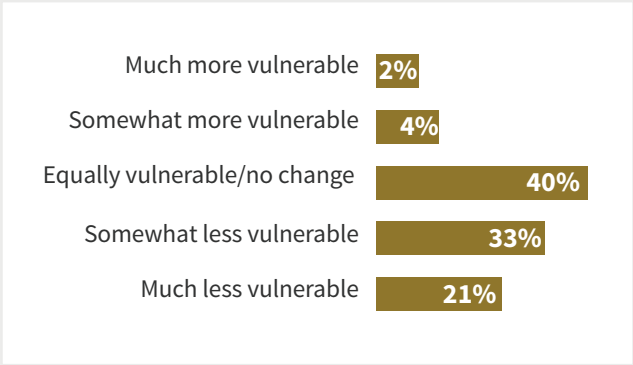
QUESTION: **In which regions does your organization operate? Data Centers; Offices; Remote Employees; Customers**

Cybersecurity and the Data Center

Changes in Organizations' Vulnerability Posture

Data centers are improving their cybersecurity posture, according to respondents of the survey.

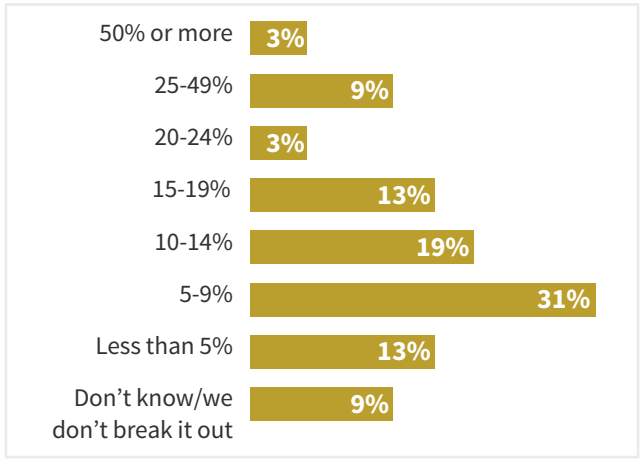
Just 6 percent said they thought their organizations were more vulnerable to cyberattacks in 2018 than they were in 2017. Forty percent said they were as vulnerable as they were before, and 54 percent said they were less vulnerable.



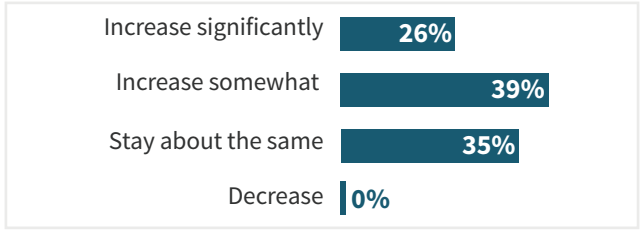
QUESTION: **Relative to 2017, how has your organization's vulnerability posture changed? In 2018 we are...**

IT Security Budget & Trends in IT Security Spending

They were also optimistic about cybersecurity budgets. None of the respondents said they expected budgets to decrease, while 65 percent expected an increase in 2018.



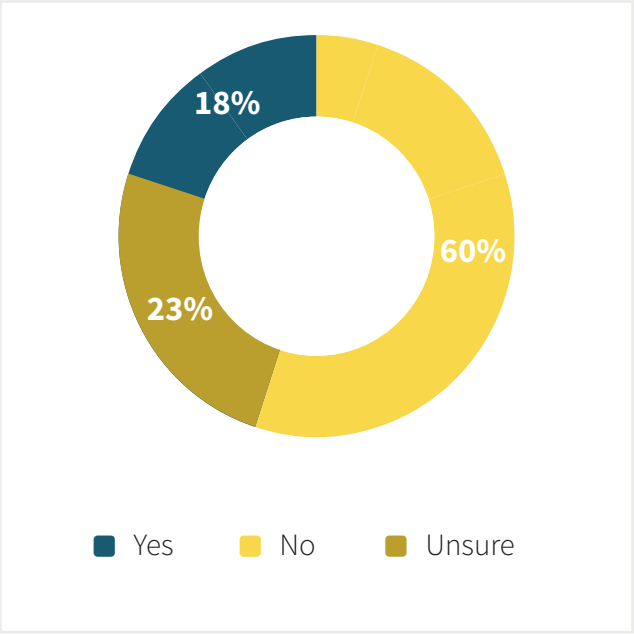
QUESTION: **Approximately what percentage of your organization's annual IT budget is allocated for IT security?**



QUESTION: **How will spending on IT or data center security in 2019 compare with 2018?**

Security Breaches Experienced in the Past Year

The majority, 60 percent, also said they didn't have a breach in 2017. Only 18 percent said they had a breach, and 23 percent didn't know.



QUESTION: **Has your organization experienced a security breach in the past year?**

According to many experts, however, data centers might not be as secure as they think they are.

Is Confidence Justified?

Marty Puranik, president and CEO at Atlantic.Net, a Florida-based data center and cloud provider, says that overall, data centers are doing a better job of protecting themselves and dealing with new vulnerabilities.

"Security has improved," he says. "But it's improved at known threats. Since the attack vectors are always changing, it's having protection from the latest attacks that is important. IT professionals are kidding themselves if they think they know about zero-day or exploits that aren't even publicly known yet."

In addition, attackers are becoming more evasive and are using new methods that aren't as easily detected, he says. Side-channel attacks, for example, are particularly difficult to stop. "Intel CPUs have side-channel attacks such as Meltdown and Spectre," he says. "At the same time, there are concerns of vendor firmware that can be taken advantage of."

Even though data centers are investing in cybersecurity and improving their data postures, that doesn't mean overall risks are reduced, says Leo Taddeo, CISO at Cyxtera Technologies, a large data center operator based in Florida. "Unfortunately for cybersecurity professionals, likelihood of occurrence is outside of their control, because they're dealing with a human adversary," he says. "While cyber defenders can reduce their vulnerabilities, they can't know whether the adversary can maneuver around their improved defenses." That's especially true for nation-state attackers, Taddeo adds.

Last December, federal prosecutors indicted two Chinese hackers known to be part of APT-10, he points out. The attackers were targeting data centers and managed services providers to get access to client data. "Given what we know about nation-states targeting infrastructure, can anyone say that they face less risk?" he says.
Syed Abdur, director of products at Brinqa, an Austin-based cybersecurity firm, also says data center managers who think they're not more vulnerable than before are kidding themselves.

"Organizations today have a lot more risks to contend with, even compared to just a few years ago," he says. "For the vast majority of organizations, their cybersecurity practices have not kept pace with this increased level of threat." Those organizations that have mature risk management capabilities and make sure of advancements in automation, orchestration and analytics are getting better at defending themselves, Abdur adds. "However, such organizations represent a small percentage."

According to the Data Center Knowledge survey, only 27 percent of respondents had automated DDoS mitigation systems and only 21 percent were using security tools enabled by artificial intelligence (AI).

Current IT Security Products Utilized

E-mail security/spam filtering	82%
Firewalls	76%
Third-party malware detection/antivirus	64%
Encryption	61%
Intrusion detection/prevention system (IDS/IPS)	52%
Data loss prevention (DLP)	48%
Identity and access management (IAM)	48%
Log management	48%
Wi-Fi access control/configuration software	48%
VPN	45%
Telephony and/or VoIP security software	39%
Cloud access security broker (CASB)	33%
Patch manager solution	33%
Automated DDos mitigation systems	27%
Web application security tools	24%
AI-enabled security tools	21%
Micro-segmentation	21%
Network admission control (NAC)	21%
Security event management/security information management (SEIM)	21%
Mobile-device-specific management: EMM, MAM, MDM	18%
Unified threat management (UTM)	15%

QUESTION: **Which IT security products are in use in your organization?**

Data center managers may also have been overconfident about whether they've had a breach or not.

"The more likely scenario is that there have been breaches and they don't know it," says Cath Goulding, head of cybersecurity at Nominet, a UK-based cybersecurity firm.

According to her, Nominet and Osterman Research recently conducted a survey of CISOs, and 60 percent said they'd found malware hiding on their networks for unknown periods of time – in some cases, for more than a year. "There's rarely an easy solution to preventing breaches," Goulding says. "Even the most reliable defenses can occasionally be penetrated."

But confidence, even if unwarranted, can be a positive thing if it helps data center managers go out and face threats every day. The opposite would be what Cisco calls "cyber fatigue" — when cybersecurity professionals have virtually given up trying to stay ahead of attackers.

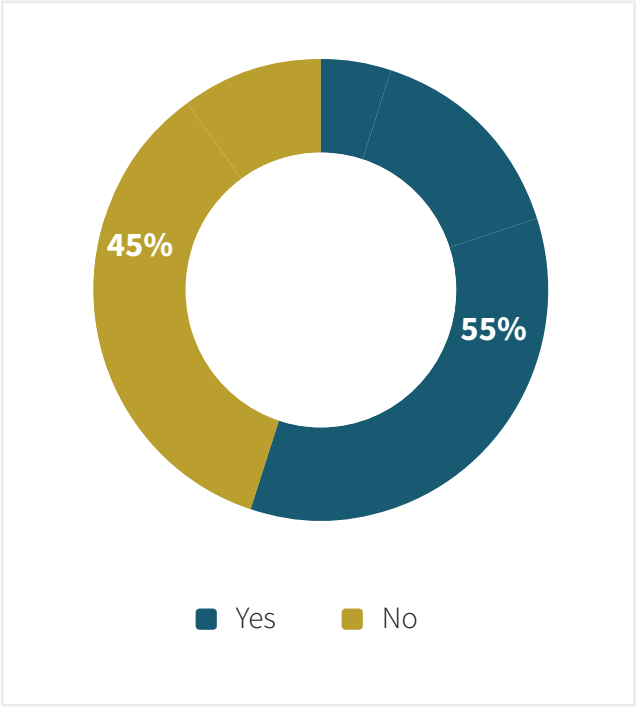
Cisco recently surveyed more than 3,000 CISOs in their annual benchmark study, and the number who said they were suffering from cyber fatigue fell from 45 percent last year to 30 percent in this year's survey.

"CISOs are feeling better about their chances," says Wendy Nather, head of advisory CISOs team for Duo Security at Cisco. "Fewer of them are giving up."

Safety in the Clouds

More than half of respondents – 55 percent – said they were using public clouds to store data, and 80 percent said clouds were as secure or more secure than their on-premises infrastructure.

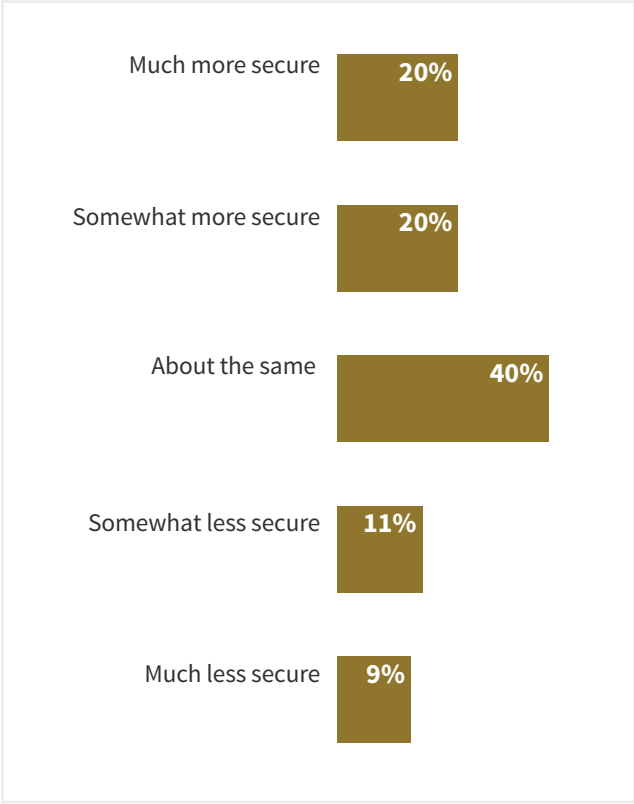
Utilizing Public Cloud Storage



QUESTION: **Does your organization store any data in the public cloud (AWS, Axure, etc.)?**

QUESTION: **Does your company have a shared security strategy for workloads running in the clouds??**

Relative Security of Workloads Running in the Cloud



QUESTION: **Compared with workloads on our own infrastructures, workloads running in the clouds are:**

Safety in the Clouds (continued)

"Cloud data centers are deploying state of the art defenses much faster than on-prem infrastructure," says Bryan Owen, cybersecurity manager at OSIsoft, a San Leandro, California-based company that provides energy management software for data centers. Plus, cloud-native systems don't have to deal with the same kind of legacy technology issues as on-premises data centers do.

For example, compatibility with legacy applications is keeping data centers from moving beyond traditional passwords, Owen says. "There are still use cases for memorized secrets, but data center infrastructure isn't one of them," he says. "Cloud-native systems have a distinct advantage."

If a data center is having trouble with patching or securely operating its firewalls, then it will definitely benefit from moving to the public cloud, says Ambuj Kumar, co-founder and CEO at Fortanix, a Mountain View, California-based security vendor. And some cloud providers are offering security capabilities that aren't available to on-prem data centers, he adds. "For example, IBM Data Shield can protect applications even when root passwords are compromised."

The cloud has become a touchpoint for security, says Andrew Howard, CTO at Phoenix-based Kudelski Security. "From our experience, we can say data center technology is generally stagnant," he says. "If you follow the product roadmaps for the major security technology providers, you will struggle to find any innovation not focused on the cloud."

However, not all cloud deployments are created equal. Cloud security company Alert Logic analyzed data from more than 4,000 customers and found that those using public clouds like Amazon Web Services and Microsoft Azure had one-third fewer security incidents than those with on-premises deployments. But those using private clouds in data centers operated by providers such as Rackspace, Hewlett Packard Enterprise, and IBM had 12 percent more security incidents, and those with hybrid cloud deployments had 60 percent more security incidents. When data centers simply migrate their infrastructure to private clouds, they're not leveraging native cloud technologies, says Jason Pfeiffer, VP of product management at ReliaQuest, a Tampa-based cybersecurity firm. "Leveraging native cloud or serverless capabilities allows organizations to take advantage of the best elements of the cloud and some of its built-in capabilities," he says. "Not to mention, the cloud providers own security that is built at scale around their entire infrastructure."

> **"The problem is endemic, and the list of enterprise IT organizations who had their private data publicly exposed in the last two years because of misconfigured AWS S3 buckets is long"** – Terry Ray

Even when cloud providers do a good job with security, it remains up to the customers to use the provided tools properly, take care of application-level security, and maintain proper access controls. News reports of AWS storage buckets storing sensitive information left unsecured, accessible via the public internet, have become commonplace. Companies that have made this mistake include Dow Jones, Accenture, Booz Allen, Verizon, Capital One and Walmart, among others.

"The problem is endemic," says Terry Ray, a Fellow at Imperva, a Redwood City, California-based cybersecurity company. On AWS alone, about 7 percent of storage buckets are configured to allow unrestricted access, he says. "And the list of enterprise IT organizations who had their private data publicly exposed in the last two years because of misconfigured AWS S3 buckets is long," he says.

Data Center Survey Reveals Cybersecurity Awareness Gaps

MARIA KOROLOV

Published October 2019

Data Center Knowledge™