CIO DIVE

TRENDLINE

Cybersecurity

Yujin Kim/CIO Dive

NOTE FROM THE EDITOR

The rush to send employees home to work obliterated the legacy security perimeter. Companies had to rethink security policies reliant on the network perimeter. There was also an influx of software to protect, as companies turned to service-based technology models.

Security threats did not dissapear with the new work constraints. Instead, CISOs watched cyberattack records shatter. The high-profile news of the SolarWinds and Log4j compromise made executives what, and who, in their supply chain they could trust.

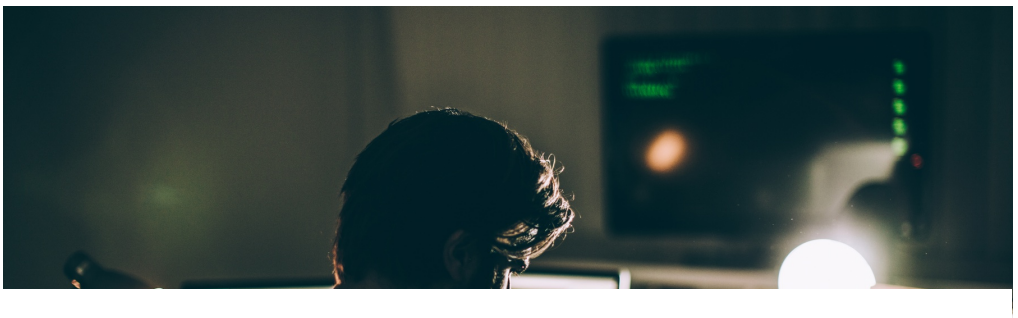
To respond, and stay protected, organizations called on savvy security leaders to help them adapt. Companies are rethinking cyberthreats in the remote work landscape, addressing long held pain points (including the ever-present thorn of terrible passwords).

CIO DIVE

ever before as international conflicts spill into the cyber domain. Security decision makers are called to defend their organizations no matter what.

The costs of failure, whether it's regulator scrutiny or tarnished reputations, are too high.

Naomi Eide
Lead Editor



Cyberthreat trends to watch in 2022

Cybercriminals are finding ways to manipulate corporate data, and for that problem, there really is no end in sight.

By: Sue Poremba • Published Jan. 31, 2022

If there is one predictable constant in cybersecurity, it's the omnipresence of ransomware. As Mandiant put it best, "There's no end in sight for ransomware."

But don't expect ransomware to continue as we know it today. Mandiant predicts threat actors will develop new ways to gain a profit from ransomware, starting with a shift to globalized attacks.

"Indictments, arrests, seizures of funds, and cyber offensive operations against threat actors and their infrastructure by U.S. law enforcement will cause threat actors to reevaluate which countries they target," said Charles Carmakal, SVP and CTO with

The common thread around these trends is cybercriminals finding a way to manipulate corporate data, and for that problem, there really is no end in sight. As 2022 unfolds, here are four cyberthreat trends to watch:

Paying ransom won't stop data publication

Paying a ransom probably won't stop threat actors from placing stolen data on the dark web or using it for extortion purposes, Mandiant warned. That's because of infighting in cybercriminal rings.

"Often, conflict arises within these groups as a specific actor may feel like they're not getting paid their fair share," said Carmakal.

To retaliate, the disgruntled threat actor in the group could decide to publish some or all of the data after the ransom is paid. As greed around ransom grows, expect it to impact post paid-ransom behavior. Individuals could break away from the group and hold the data ransom multiple times.

"The more this happens, the more it's going to affect the way organizations think about making ransom payments," said Carmakal.

Ransomware as espionage

There has been at least one international cyberattack conducted as an act of espionage in 2022. As tensions between countries escalate, Carmakal also anticipates governments will leverage ransomware in extortion operations.

Threat actors will use masquerading ransom or extortion operations to disguise the objectives of some intrusions, especially when there is conflict between nations.

Attacks on the software supply chain

This year, cybersecurity experts are sounding the alarm on attacks

"Log4j is not the first or last software supply chain vulnerability, but it is by far the most widespread and easy to exploit weakness that we've seen in many years — including SolarWinds," said Kumar Saurabh, CEO and co-founder of LogicHub.

The Log4j vulnerability impacted the logging feature of Java, which runs on billions of devices, especially internet of things (IoT) devices, many of which have some form of logging enabled. Seeing how vulnerable these ubiquitous and often ignored codes are in open source software, threat actors will up the ante and go after other forgotten code to exploit.

"What's critical now is careful monitoring of logs from all possible security tools. Unfortunately, many security teams are already flooded with security alerts, and often don't monitor all logs because of excessive storage costs with many SIEM tools," Saurabh.

It is another type of attack that could be attractive to nation-states looking to infiltrate governments or wreak havoc on the systems that control the critical infrastructure. A powerful zero-day exploit can fetch top dollar on the black market, but it might be worth even more if it remains closely guarded in the toolbox of a sophisticated APT team, including those sponsored by a nation-state, ready to be deployed surgically without attracting too much attention.

SMBs lack the manpower for in-house monitoring or keeping track of the open source software supply chain. Nor can they analyze or reverse-engineer every software update a vendor sends them. Zero trust models may be the ultimate solution for this style of attack.

"Adopting the ‘assumption of breach' philosophy combined with an asset-based risk management and risk transfer program may be the only way to keep up with the bad guys," said Daniel Schwalbe, CISO at DomainTools.

While many cybercriminals tend to pursue high-profile attacks designed for financial gain, threat actors are increasingly trying to infiltrate companies and go unnoticed for a long period of time. These quiet attacks allow cybercriminals to exfiltrate data from servers and endpoints at a slow and steady pace.

In today's hybrid/remote work reality, the information on remote computers is typically less protected, putting it at higher risk for a stealth attack.

"Quiet threats are on the rise because cybercriminals are well aware of the value of data to business and other organizations," said Nigel Thorpe, technical director at SecureAge.

In 2022, expect email and other messaging systems to be the most popular point of entry for these quiet attacks, with the goal of compromising corporate communication systems. Cybercriminals can then infiltrate the corporate network and do damage from the inside without discovery.

Article top image credit: South_agency via Getty Images

Ukraine conflict spotlights business need for cyber resilience

In the crosshairs: critical infrastructure and companies with global operations.

What the world saw: a land, air and sea attack by Russian forces into Ukraine. What enterprise IT executives heard: cyber risk is level red.

Modern IT and supply chains are interlinked, and recent attacks have shown the potential financial and physical consequences. Military operations and cyberattacks on Ukrainian government agencies and high-profile companies telegraphed a clear and present danger, especially for infrastructure and global businesses.

"Ukraine has been the target of past and ongoing episodes of disruptive cyberattacks, which governments and cybersecurity experts have attributed to the Russian government," according to a research note from Moody's Investors Service. The firm is concerned over the consequences of a digitized and interconnected IT ecosystem, which — in the event of an attack — can trickle across sectors and geographies.

Information sharing and cross C-suite communication can help decrease cyber risk. Security research firms are also watching for the spread of a destructive data wiper malware.

"Organizations need to lower their thresholds for escalating anomalous activity and sharing that information with the government," said Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency, speaking in February before the Aspen Institute.

Experts are on alert for cyberattacks because of past disruption from the NotPetya malware strain, which initially targeted organizations in Ukraine. The malware attack led to billions of dollars in damages for companies internationally.

"I definitely would consider that a watershed event, not just from the cyberattack perspective," said Luke Tenery, partner at global advisory firm StoneTurn. "We obviously saw what a nation state could do on a number of levels. That incident caused ripple effects also across broader industry, disabling a number of global organizations that impacted supply chain, and other aspects of

CIO DIVE

What risk preparedness looks like

In cybersecurity, prevention and rapid security response starts with information.

"CIOs that are able to not just consume the information, but then integrate it to make it part of how they manage risk are the ones that are going to do probably the best out of all this," Tenery said.

For firms sourcing IT from providers in the region, it is critically important to review communication frameworks and have an ongoing review of how the crisis could impact operations.

"No. 1 is communication," said Stanton Jones, director and principal analyst at ISG. Senior leaders from supplier and buyer side need to have regular communication to ensure continuity."

In the face of live fire in Ukraine and decaying diplomacy, firms should have fallback plans to ensure continuity.

"There absolutely is a geopolitical threat, and obviously it appears to be worsening very quickly," said Jones. "But many of these firms are well prepared for it and have either started moving work out of the country, or moving teams out of the country."

Article top image credit: Chris McGrath via Getty Images

CIODIVE

How Log4j is shaping enterprise security strategies

Federal officials warned companies of the long-term implications of Log4j. Leaders are taking internal steps to keep threat actors at bay.

By: Roberto Torres • Published Jan. 27, 2022

The Log4j vulnerability emerged as a critical cybersecurity risk factor at the end of 2021, threatening to leave millions of devices open to attack.

The scope of the flaw, which targets a widely used Java-based logging utility, is pushing IT executives to reassess how they protect systems and shore up defenses against open source vulnerabilities.

Though many businesses quickly patched their systems, the threat of Log4j looms large in 2022. Sophisticated threat actors could be waiting to use the exploit, catching targets in a lower level of awareness, according to Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency (CISA).

Tech executives can guide how their businesses respond, recover and prepare for future threats. Half of CIOs will prioritize security management in 2022 as CEOs seek to lower risk exposure, according to an IDG report. Cybersecurity also gained relevance for boards of directors, a response to the the increasing threat of operational disruption.

For CIOs, Log4j tested the role tech leaders play in cybersecurity response, from collaborating with other C-suite members to addressing the technical challenges of remediation.

"The first piece I think is pretty standard across most organizations: learning about the vulnerability, identifying which systems are impacted and patching as quickly as possible," said Blumofe.

The company used third-party tools and in-house products to detect vulnerable Java applications, and relied on its Web Application Firewall (WAF) to provide protection and allow patching to take place under less pressure.

Each company addressed the vulnerability according to its own roadmap, but speed is one common element.

Global Payments took swift action to respond to the vulnerability, said Guido Sacchi, SEVP and CIO.

"All our systems have been patched and brought up to speed with the latest upgrades," said Sacchi. "There's been a lot of work just to make sure that our systems are taken care of.

In addition to updating its WAFs, Global Payments ran indicators of compromise through its system, relying on information from the Financial Services Information Sharing and Analysis Center to ensure there were no signs of compromise.

Security posture adjustment

The massive scope of the Log4j vulnerability is pushing leaders to revisit their security products and remediation tactics, alongside their security stance ahead of possible future risk.

Global Payments took a close look at possible cyber risks coming in undetected from the vendor side.

"We have a very mature vendor management program, and follow up directly with vendors to make sure what's present in our infrastructure is taken care of," Facchi said.

Akamai relies on zero trust to reduce the possibility of compromise, according to Blumofe. Under this approach, each

"We expect this approach to greatly reduce the threat surface when a vulnerability arises," said Blumofe. "And in many cases, [it can] stop the attack chain before we are impacted."

Article top image credit: anyaberkut via Getty Images

Want to quickly recover from ransomware? Plan ahead

Security teams need to understand how the business will work when an attacker limits access to its systems.

By: Katie Malone • Published July 15, 2021

When a ransomware attack hits a business, the recovery doesn't stop at the decision of whether to pay the ransom.

For businesses, the first step post-hack is to contain the attack. "Evaluate systems that have been affected ... [by] the attack and then look to contain and limit that attack," said Asher de Metz, senior manager of security consulting at Sungard AS. "Then once it's contained, they're also going to want to communicate with stakeholders."

Consider the recent Kaseya attack: After triaging and releasing a patch for on-premise customers, the company still had to mitigate the SaaS damage with a separate patch. Weeks after the attack,

With some hindsight, researchers are uncovering where Kaseya went wrong and what the company could've done differently to prevent the attack affecting 1,500 downstream customers. But for businesses watching the drama unfold as another company scrambles with a post-hack response, the lesson is to prepare for the worst.

"The most critical factor is completely eradicating the threat from the environment," Tim Grelling, director of innovation, security at Core BTS, said in an email to Cybersecurity Dive. "Attempts to 'uninstall' or clean ransomware from systems is rarely successful."

Because of the sprawling damage, recovering from a ransomware attack can be pricey. The average total cost of recovery from a ransomware attack was $1.85 million in 2021, according to a Sophos report.

Post-attack recovery actually begins before a cyber incident ever occurs. Drafting an incident response plan, practicing response tactics and making sure the systems are in place for a full recovery should happen before the attack as a part of the recovery process.

"Businesses that use the lessons learned from the incident and use them to not just restore services but improve their security policies, processes, tools and architecture will come out of the incident with something positive if they maintain the improved security posture," Grelling said.

When an attack first happens, the security team will lead a business's incident response to contain the issue and stop the bleeding, according to Mark Nunnikhoven, distinguished cloud strategist at Lacework. Most of the time, the decryption will get the data back, but there's still the possibility of corruption and whether back-ups are available in the meantime to restore systems.

Then, the unknowns set in. "Are we still vulnerable? Did we remove all of the malware and things that the attacker did from our network? It's a really long and drawn out process,"

The challenge for businesses is managing the scale and scope of the attack. When attackers have access to the network, they take advantage of it to understand where the more important data is, according to Nunnikhoven. The business has to determine how the attacker got in and also trace for any additional damage or unwarranted access.

'Plan, plan, plan'

For a strong post-hack comeback, planning is required.

Two-thirds of companies estimate it would take five or more days to fully recover from a ransomware attack if they chose not to pay the ransom, according to the 2020 Ransomware Resiliency Report surveying 2,690 IT professionals. A similar number, 64%, say their security measures have not fully kept up with their IT complexity.

"The first step is, have a plan ahead of time. I know that sounds simple, but so many people don't do it," Nunnikhoven said. "You need to understand how you're going to work if you don't have access to your systems."

In combination with a plan, good cyber hygiene across the business can be preventative and help quickly respond to cyberthreats. For example, businesses can roll out patches more quickly without a massive effort, Nunnikhoven said.

Because of the string of recent high-profile attacks up the supply chain, incident response plans and preparation now include vendors in the process.

"Supply chain attacks have increased the focus on third-party risk management," Grelling said. "Businesses need to not only manage security and risk in their own environment, but identify those critical vendors and assess security and risk related to those vendors."

If an organization has a strong incident response plan in place — and has spent time practicing it — they'll likely be more successful

CIO DIVE

"Plan, plan, plan," de Metz said. It's worth it to a business to spend the money now on the preventative measures because ransomware can be incredibly destructive.

Article top image credit: Alex Wong via Getty Images

Security strategies evolve while spending flatlines

Organizations want more bang for their buck, which can mean eschewing single-use products.

By: Brian Eastwood • Published Feb. 9, 2022

Surprisingly, IT security spending has been flat for several years, recent data from Gartner show, but that doesn't mean organizations are standing still.

Investment in new security products and the emergence of leadership roles beyond the IT department suggest security is still gaining visibility at the C-suite and board levels.

By two measures – the portion of IT spending on security and IT security spending per employee – spending has stagnated since 2016.

Last year, the median level of spending on IT security accounted for just 5% of total IT spending, up slightly from 4.8% in 2017.

revenue increased, though that's largely due to declining revenue in 2020.)

For Gartner, these figures represent a baseline, as the firm expects IT spending and IT security spending to continue to grow in tandem.

"We don't see things slowing down in any significant way," said Nat Smith, senior research director with Gartner.

Spending the same amount, only on different products

Where IT security spending has shifted is in the type of IT asset it protects. From 2019 to 2021, spending on security for hardware dropped to 10% from 15%, with spending on security for software increasing to 32% from 27%.

The reason: cloud.

"Organizations want to see how vulnerable their pieces of the cloud are," he said.

Companies are pouring money into products such as cloud entitlement management, which helps manage permissions, and cloud security posture management, which identifies cloud misconfigurations and other compliance risks.

Organizations are also looking to get more for their dollar, which can mean eschewing single-use products.

Secure access service edge, for example, consolidates several security functions — including SD-WAN, VPN, firewall and zero-trust access — into a single cloud-based service.

Meanwhile, identity products often bring together governance and administration, single sign-on, access management, and multifactor authentication.

For all the evolution in spending strategy, there's a catch. Organizations that have experienced a security breach or another incident are more likely to spend – and spend wisely – than those

Group.

After your company has been breached "you have a lot of buying power, and you're not working as hard to justify your investments," she said. Before a breach, "There's a false sense of complacency. Even if the security lead says, ‘We should be spending more.' Ultimately the person responsible is the CFO or someone who isn't a security leader. To them, it's not a priority."

Security a business, not just IT, function

Changing this perception is no small task, Hertanto said. Trusting relationships between security leaders and the rest of the executive team, as well as the Board of Directors, play an important role.

"You can't expect to convince them in a half-hour board presentation. It takes years to build that trust," she said.

Increased understanding that security is an independent business function, and not just an IT function, helps to close that gap.

Gartner projects that a single executive focused on security – namely, the CISO – will be insufficient for most large organizations as early as 2025.

Additional roles may include a chief risk officer, who manages the overall risk of business assets, or a cyber risk officer, who assesses risks such as breaches, data leaks, or cloud misconfigurations in the software products.

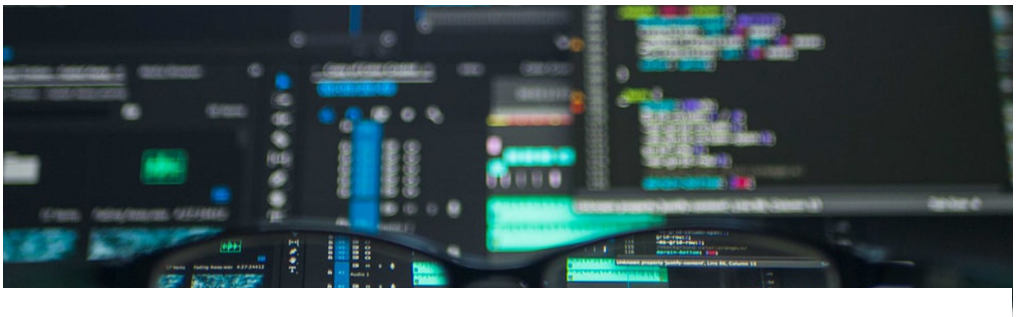
Software vendors may also consider a product security officer tasked with understanding the inherent risks in the products the company ships, such as any third-party resources.

With these new roles, IT security spending will move to other business units. This will force organizations to look at security in the context of business priorities, according to Hertanto.

The time is ripe to shift the perception of security as "The

"In many organizations, security is still seen as a business cost center, going against innovation and impeding growth. But security can be a business enabler," Hertanto said. "If you don't manage business risks accordingly, you can't achieve greater gains. Security can be an enabler in the same way."

Article top image credit: AzmanL via Getty Images



6 types of CISO and the companies they thrive in

Jeff Pollard, VP and principal analyst at Forrester, wants CISOs to discover the type of leader they are — transformational, tactical, steady — and run with it.

By: Samantha Ann Schwartz • Published Sept. 22, 2020

As with many cybersecurity professionals, some CISOs were "accidented" into the role, said Jeff Pollard, Forrester VP and principal analyst, while speaking at the virtual Forrester Security and Risk Global 2020 conference. But as the CISO role evolves and takes shape, the decisions they make and projects they oversee will become more intentional.

Security is involved in privacy, legal, productivity, breaches, threats, software — CISOs have their hands in everything. But as the CISO's plate is overloaded with responsibility, they become a master of none, to the detriment of the company.

leaders have had to do.

Today's CISO faces a daily inundation of competing priorities, forcing them to table projects and make tradeoffs.

Only 13% of CISOs are considered C-suite executives, up from 5% or 6% a couple years ago, according to Forrester research. The rest of security leaders are referred to as VPs or directors at Fortune 500 companies.

Of that 13% of CISOs, most are on their third or fourth CISO job, said Pollard. This indicates that they were experienced enough to advocate for that seat at the C-suite table.

The CISOs that overcome the challenges of the role — accidental appointment, overwhelming responsibility, and limitations of authority — should "fire themselves," said Pollard. Pollard wants CISOs to rid themselves of activities they don't need to do. "You'll feel like you're losing valuable stuff, but it sets you free."

Flavor of the week

There are six types of CISOs depending on the type of organization they work and their personality type, according to Forrester:

1. Transformational: Often "energized" to dive into a three- to five-year transformational initiative, said Pollard. These individuals tend to enjoy turn-around projects and watching business outcomes unfold.

2. Post-breach: Thrive in turbulence; they take on rebuilding a company's security organization while mitigation and PR crises play out in the background. These CISOs don't mind the possibility of becoming "the punching bag" for vendor presentations in the future, said Pollard.

3. Compliance guru: Typically work in highly regulated industries and are fluent in regulatory bodies and acronyms: HIPAA, CCPA, FDA, etc.

5. Steady state: One of Pollard's favorite types because they usually serve at companies that don't need immediate transformation. "Maybe the company is OK right now," he said.

6. Customer-facing/evangelist: Unafraid, and rather enjoys being their company's spokesperson for cybersecurity. Tech companies often have this kind of CISO because they can appeal to customers with their charisma.

All CISOs face burnout because they might be in an imperfect match with their company.

A transformational CISO will not thrive in a steady state company, and the disconnect will lead to a poor security culture. But that's not to say CISO types can perform in different kinds of companies.

Post-breach CISOs typically leave after three years of cleanup. By this point, the breached company will want a steady state or tactical CISO to carry on security duties.

"It's interesting, after a breach, one of the major changes organizations will implement is a change to the CISO role," said Stephanie Balaouras, VP and group director at Forrester, in the comment section of the livestreamed session.

Post-breach companies will either hire "a dedicated CISO if they didn't have one, [moving] the reporting relationship to higher in the organization, even outside IT and into the CEO," said Balaouras. The reporting structure for CISOs might also shape their next career move.

"We had a CISO tell us they were in a board meeting. They asked the CIO to leave the room while the CISO met with the board so there was no conflict," said Pollard. If a current CISO doesn't see eye to eye with their CIO, they can eventually become one.

Article top image credit: Kevin Ku for Unsplash

CIO DIVE

Employees can't quit habit of writing down, sharing passwords

By: David Jones • Published April 6, 2021

Amid a growing debate about cyber hygiene practices and insider threats, the majority of corporate workers in the U.S. engaged in sloppy management of work-related passwords, according to a report released Tuesday by Keeper Security. Conducted by Pollfish, the research was based on a survey of 1,000 corporate workers.

The report shows 57% of U.S.-based corporate employees are writing passwords on sticky notes. Two-thirds of those surveyed lost the written down passwords in the past, raising questions about who actually took possession of them.

In addition, 62% of respondents said they have shared a work-related password over email or text message, which are vulnerable to cybertheft. About 46% of respondents said their company directed them to share passwords that are used by multiple people.

The report comes at a time of robust debate about password security practices and cyber hygiene in the U.S. technology sector, critical infrastructure entities and government agencies across the country.

SolarWinds, a central player in the nation-state attack against the U.S. last year, was blasted by lawmakers during February Congressional hearings amid reports that "solarwinds123" had been used as a password internally.

inadvertent and purposeful data leaks, according to a report released in March by the Ponemon Institute on behalf of Code42.

The year-long move to remote work following the outbreak of COVID-19, appears to have accelerated already weak policies and practices of these entities, as about two-thirds of workers said they were more likely to write down passwords when they were operating from their home environments, according to the report.

"For some reason, when people move to a remote work setting, they're more lax about their password security, and they're more prone to violate or soften internal controls with respect to their employers," Darren Guccione, co-founder and CEO at Keeper Security, said in an interview.

Besides the storage of passwords, a significant percentage of workers are making poor decisions about their creation of new passwords. About 37% of respondents said they incorporated their company's name into a password and 44% are using the same password for work and personal accounts.

Article top image credit: SARINYAPINNGAM via Getty Images

CIO DIVE

CEOs target risk reduction

An IDG survey found security improvements are driving IT budget increases.

By: Samantha Ann Schwartz • Published Jan. 27, 2022

Half of CIOs are prioritizing security management this year, as CEOs push for IT and data security upgrades to reduce corporate risk, according to IDG's annual CIO survey, which included responses from almost 1,000 heads of IT and 250 line of business participants.

Increasing cybersecurity protections is the top business initiative for 2022, especially for IT leaders in the government, education, manufacturing and healthcare sectors. Respondents cited socioeconomic factors for driving focus on security, the report said.

The majority of IT leaders, 76%, expect to be more involved in cybersecurity this year, while maintaining their role as the primary technology decision maker, the report said. This is particularly for CIOs in government, healthcare and manufacturing. Security and risk management skills are also the top skills CIOs are expected to seek this year.

Without visibility into a company's tech stack, a CISO's ability to defend a network is weakened. Software complexity is a top challenge for CIOs and CISOs.

The reporting structure between CIOs and CISOs varies. With IT and security demands sometimes at odds, many CISOs report directly to the CEO. However, a direct CIO to CISO rapport gives leaders insights into the network and what is necessary to defend it.

The majority of CIOs engage with their CEOs more than other C-suite executives, while engagement is evenly split between CISOs and CTOs, a 2021 IBM report found. The survey was based on 2,500 responses from CIOs and 2,500 responses from CTOs

IBM found that cybersecurity is among the shared responsibilities of the CIO and CTO.

Nearly three in five respondents (57%) cited security improvements as a driver for their budget increases this year, according to IDG. The top technology investments for 2022 are in security and risk management, followed by data and business analytics, and application and legacy system modernization. Upgrades to IT infrastructure came second to security improvements as reasons for budget increases, IDG found.

The increased focus on cybersecurity can bridge potential technological gaps between IT and the security organization. SolarWinds, for example, is a tool CIOs were likely familiar with, Chris Krebs, former director of the Cybersecurity and Infrastructure Security Agency (CISA), said during a virtual Gartner conference in October. CISOs "may not have had as deep an understanding of the Orion product and platform," the software's criticality in maintaining network operations, Krebs said.

CIOs and CISOs play equal roles in defensive collaboration — each has a responsibility to demand higher security standards from the vendors they work with. CISOs have the responsibility of shedding light on risk, not necessarily security practices for their C-suite counterparts.

Article top image credit: "wocintech (microsoft) - 112" by WOCinTech Chat is licensed under CC BY 2.0

CIO DIVE

Security hampers enterprise cloud adoption

Multicloud adoption adds complexity as IT security teams struggle with alert fatigue.

By: David Jones • Published Feb. 23, 2022

Cybersecurity is the leading obstacle for expanded cloud and multicloud adoption, the top concern for more than two-thirds of IT leaders, according to a study released by Confluera. The company commissioned a survey of 200 IT leaders and medium and large organizations, using an independent research firm.

IT teams spend over half of their time investigating cybersecurity alerts, however more than half of these alerts are either false alarms or otherwise considered benign threats, according to the report.

The increased demand for cloud deployments due to remote work, coupled with the heightened pressure on IT security teams amid record job resignations, has led to increased fatigue and job burnout.

Organizations have raised security concerns when they expand the number of cloud deployments. The reliance on a multicloud environment, using some combination of infrastructure as a service (IaaS) providers, including Google Cloud, Amazon Web Services or Microsoft Azure, complicates the security dynamic.

The report shows 97% of IT leaders are expanding cloud adoption at their organizations as part of internal strategy. Meanwhile, almost 70% of respondents were concerned about consistent security coverage when operating across different cloud

CIO DIVE

2021 represented the first full year for many companies in terms of supporting a newly remote workforce, according to Confluera CEO John Morgan. Many IT security officials expected to focus on securing remote devices and insecure network connections, Morgan said.

"The reality is that IT professionals spend the most time and are most burdened by the adoption of cloud services, which is more of a backend infrastructure," Morgan said via email.

Prior research studies illustrate the complexity of securing a remote workforce, as well as an increasing visibility gap inside of cloud infrastructures.

A 2020 buyer survey from Gartner showed more than three-quarters of organizations were adopting a multicloud infrastructure. But different providers supporting different sets of policies makes it difficult for many companies to create a consistent security posture, an October 2021 technology trends report from Gartner shows.

"The biggest challenge around the security of multicloud for enterprises is that all cloud providers and services are not providing the same levels of maturity in their features," said Patrick Hevesi, research VP at Gartner. "Then when you factor in large numbers of cloud apps, the complexity of trying to map and secure each of them is overwhelming for the security team."

Article top image credit: luza studios via Getty Images