2022 Cybersecurity Year in Review:

Everything, Everywhere, All at Once

Sponsored by

RSAConference™

CRA Business Intelligence | SC MEDIA

Contents

Cyberattacks raged in 2022, but security teams made progress

Cyber attackers capitalized on security vulnerabilities that were created as companies rushed to enable cloud-based, remote operations. But along the way, security teams improved their ability to fight back.

The past two years changed how organizations all over the world conduct business. Across countries and industries, employees quit their jobs, leaving organizations vulnerable in their absence.

They relocated with little to no notice, creating secure access headaches for IT security teams, and adjusted to digital services that minimize human contact to curb the spread of COVID.

Nearly every nation continues to contend with COVID surges that periodically disrupt daily life due to ongoing supply chain and workforce shortages. Companies now must also question how much to trust third-party partners brought in to fill gaps or foster growth.

In 2020, the world panicked, then pivoted to survive (both literally and figuratively). Digital transformations accelerated and expectations evolved. So did threats targeting organizations still transitioning to a new way of working. That includes information security specialists responsible for protecting the systems, networks, data centers, and technologies that fuel today's economies. In 2021, the world adapted to a hybrid workforce but struggled to keep up with the expanded threat landscape it created. In 2022, organizations suffered the headaches that come with this new world and struggled to find the way forward.

But with tools and frameworks like zero trust, XDR and more automated threat intelligence tech to bolster vulnerability management, cloud, email and endpoint security, organizations fought back – and established plans to invest more to secure networks and data in the next two years.

Here are 7 key areas where security practitioners struggled and, in many cases, made headway, based on their participation in CyberRisk Alliance Business Intelligence (CRA BI) surveys conducted throughout 2022:

Companies scrambled to address pandemic-era cloud security gaps

Security executives recognize that most business technology systems will be maintained in a cloud environment moving forward. But in 2022, the way forward was littered with hazards.

An October 2022 article in SC Media captured the risk, noting that the average company possessed 157,000 sensitive records exposed to everyone on the internet by SaaS app sharing features, representing $28 million in data-breach risk. Also in October, security vendor Proofpoint reported that 2021 data from its customer base showed troubling trends: more than 90% of monitored cloud tenants were targeted every month, with some 24% successfully attacked.

Indeed, the last year demonstrated the dramatic and costly ramifications that typically result when organizations fail to address security as part of larger, IT-driven evolutions in how they operate.

Security an afterthought amid rapid shift to cloud

When companies rushed into the cloud at the start of the pandemic, the focus was to simply keep business afloat and provide employees with the ability to work from home. In the emergency, security often wasn't top of mind. Throughout 2022, security practitioners acknowledged the security risks.

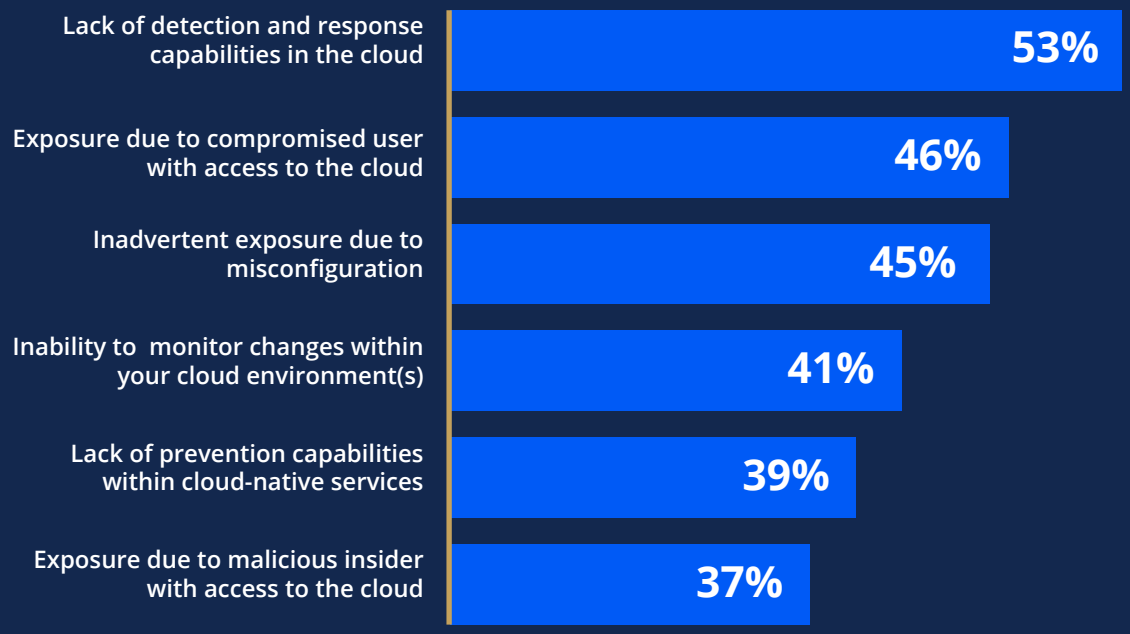
Cloud Security Alliance (CSA) researchers reported that only 39% of organizations surveyed said they had high levels of confidence in their ability to secure cloud data, while only 4% reported sufficient security for 100% of their data in the cloud. The survey also found that third parties, contractors, and suppliers are the most-commonly-targeted groups (58%) in cyberattacks. And some 92% that have already experienced a data breach believe they will experience another breach of cloud data in the next 12 months.

The CSA findings were similar to those in a May 2022 CRA BI survey of more than 300 IT and cybersecurity decision-makers and influencers in the United States. Respondents warned that, even as some organizations learned and adopted "cloud-first" frameworks and procedures, others simply lifted and shifted their current applications to the cloud with little to no customization, creating the potential for significant long-term risks to their security posture.

As a result, 37% of respondents reported their organization experienced a cloud-based attack or breach in the last two years. On average, this amounted to four attacks per victim since 2020. As cloud-based assets/workloads increased, 50% of respondents were very concerned about their ability to secure their cloud systems, with 72% "extremely" or "very" concerned.

Understandably, increased reliance on cloud environments brought heightened concern. According to the survey, 55% of respondents said they were running up to 50 assets/workloads in the public cloud and 56% on hosted clouds; on average respondents maintained 66 assets in either public or hosted clouds. Specifically, the surge translated in the eyes of security practitioners to increased risk of misconfiguration, depleted detection and response capabilities, and oversight challenges.

What are your top three security concerns about data stored in your cloud environment(s)?



CRA Business Intelligence Survey, April 2022.

Trends impacting “cloud-first” and lift-and-shift

	CLOUD FIRST / CLOUD NATIVE ADOPTERS*	LIFT AND SHIFT CLOUD ADOPTERS*
Average number of cloud assets	Public Cloud: 83 Hosted Cloud: 70	Public Cloud: 61 Hosted Cloud: 63
Average number of cloud attacks or breaches in past 2 years	3.3	2.7
Top 3 security concerns	■ Inadvertent exposure due to misconfiguration (48%) ■ Inability to monitor changes within Cloud environment(s) (47%) ■ Lack of prevention capabilities within Cloud-native services (46%)	■ Lack of detection and response capabilities in the cloud (52%) ■ Inadvertent exposure due to misconfiguration (47%) ■ Exposure due to compromised user with access to the cloud (45%)
Top 3 drivers of cloud strategy	■ Business requirements (63%) ■ IT/development demands (63%) ■ Regulatory requirements (39%)	■ IT/development demands (67%) ■ Business requirements (55%) ■ Regulatory requirements (42%)
Most likely to be included in cloud security strategy**	■ API Security ■ Cloud Workload Protection Platform ■ Container Security ■ Infrastructure as Code ■ Penetration Testing ■ Software Composition Analysis ■ Static Analysis Security Testing ■ Vulnerability Management	■ API Security ■ Cloud Workload Protection Platform ■ Infrastructure as Code ■ Vulnerability Management
% indicating very high confidence in securing cloud	33%	20%
% indicating increased spending In 2022 since 2021	89%	93%

* Predominantly large organizations (1,000+ employees)
** Cited by at least 50% of respondents

More vulnerabilities = more data breaches

In 2022, headlines about data breaches enabled by cloud vulnerabilities appeared almost daily. As recently as October, in fact, SOCRadar reported that their cloud security monitoring platform identified an exposed Microsoft Azure Blob server bucket that contained sensitive, non-public data for more than 65,000 Microsoft customers across 111 countries. The company said the leak, which they called BlueBleed, included proofs of concept and statements of work, personally identifiable information, intellectual property, product orders, project details and other user information.

Furthermore, 2022 demonstrated how companies can be held responsible for such breaches, if deemed to be the result of failure to effectively secure cloud environments. Consider the grocery chain Wegmans, which in late June was hit with a $400,000 fine imposed by the New York State Attorney General for allegedly exposing the personal information of some 3 million shoppers. The AG said the company kept information, such as addresses and driver's license numbers, in cloud storage containers that were misconfigured for over three years, during which time a bad actor could have easily cracked the login and made off with the data.

As stated in the ruling, there is "no excuse" in the 20th century for companies to have subpar cybersecurity systems.

The lesson: Much like email-based phishing and malware delivery, attempted cloud account compromise has developed into a substantial and permanent feature of the threat landscape, and companies that fail to address risks can face significant consequences.

The path to cloud security

The news wasn't all doom and gloom, however. Challenges aside, some respondents of the CRA BI survey expressed hope for real progress in their cloud security initiatives in 2022 and beyond. Ninety percent reported plans to spend 3-10% more on cloud defenses than they had in 2021 – an encouraging sign of recognition not only by security leaders but boards and executive teams that typically influence the purse strings.

Zero trust adoption lagged as orgs struggled with concepts

Massive security vendor hype surrounded zero trust in recent years, with many claiming to have the solutions to enable zero trust out of the box. Given the market saturation – and a mandate from the Biden Administration for federal agencies to implement zero trust – one could reasonably expect most organizations to be well on their way. But in 2022, organizations instead found themselves caught in stiff headwinds.

This was especially true for federal agencies. In June, for example, the Center for Strategic and International Studies released a report that took a hard look at the implementation challenges surrounding zero trust efforts, which included things like encryption, multi-factor authentication and improved logging that should have been done years ago.

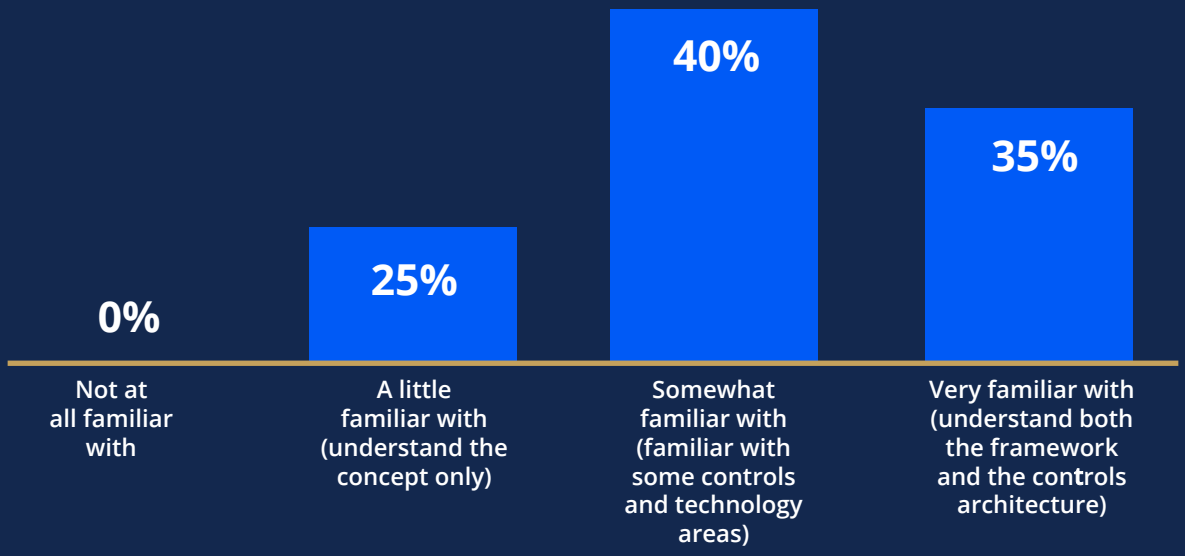
Similarly, a September 2022 CRA BI survey of 216 security practitioners found those difficulties affecting organizations across multiple industries. Respondents described a host of challenges slowing their integration of existing systems into an overall zero-trust framework, including the shift from a legacy "all access" identity and access model to one that is limited to just what is needed.

Zero trust gridlock

During the study, only one out of four respondents reported their organization had implemented zero trust.

Those who hadn't made the leap to zero trust in 2022 said the transition was just too difficult and wouldn't be effective at their organization. Others said budget limitations and inadequate staff to provide oversight or support for a zero-trust model kept them from adopting it. The most prevalent obstacles in adopting zero trust, however, were the lack of knowledge about the framework and lack of buy-in from senior management.

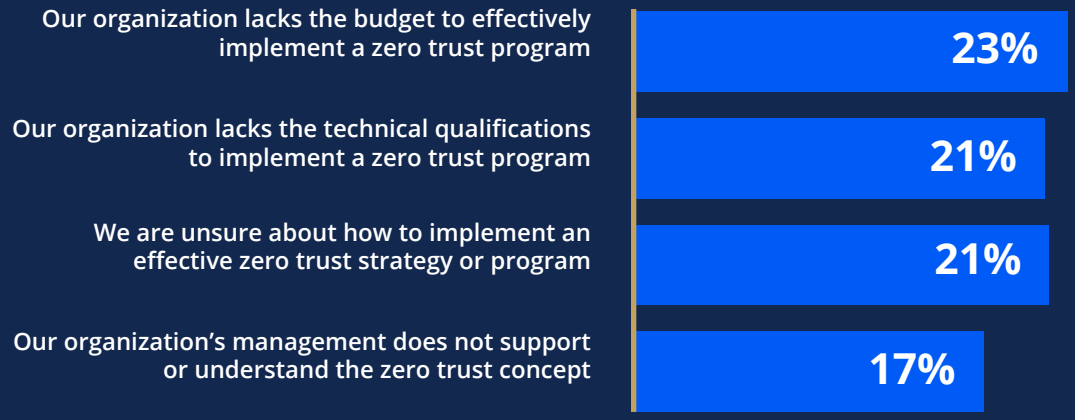
Which of the following best describes your familiarity with the zero trust security model?



CRA Business Intelligence Survey, February 2022.

How much do you agree or disagree with each of the following statements about zero trust? Rate each on a scale from 1 to 7, where 1 is “strongly disagree” and 7 is “strongly agree".

(% of respondents who rated each 6 or 7)



CRA Business Intelligence Survey, February 2022.

As one respondent put it, “Technical execution seems to be the most challenging part. Making sure we’re able to gracefully convert from a trusted environment to zero trust is what’s taking the most time.”

An SC Media article about zero trust efforts among federal agencies noted that initiatives were clashing with long-standing cultural and budgetary problems plaguing federal IT teams, a problem shared by the CRA survey respondents from other industries.

Said Suzanne Spaulding, former head of CISA’s predecessor agency the National Programs and Protection Directorate: “We have a tension here, because part of what we also need to do is make sure Congress really gets it that this is a multi-year effort and that they can’t be demanding [at the end of this year] ‘Why haven’t you migrated completely to a zero-trust architecture yet?’”

Zero trust successes

Despite the headwinds, the news about zero trust in 2022 wasn’t all bad. Leading the way in implementation were organizations CRA BI called “zero trust champions.”

In September, slightly more than half of respondents fit the champion mold based on their status for implementing zero trust and their overall perception of its importance in their zero-trust strategy.

Zero trust champions...

Are zero trust implementers (47%) or planners/evaluators (45%)

Are more likely to believe zero trust is a very important (54%) or extremely important (43%) component of their organization's overall cybersecurity strategy

Two out of three (65%) are driven by data protection as their top motivator for zero trust

A large majority currently implement zero trust to verify identity (83%)

Nearly three out of four (72%) are enterprises with 1,000 or more employees

Nearly half (48%) have large IT security teams (11 or more staff members)

High tech, financial services and manufacturing industries make up more than half (52%) of all Champions

The "zero trust Champions" segment is based on a K-means clustering model developed from the September 2022 zero trust survey data.

Meanwhile, even among those who face zero-trust headwinds, plans were afoot to ramp up spending on zero trust expertise and technology. The challenges are many, but most organizations expressed a determination to ultimately adopt zero trust in 2023 and beyond.

In October 2022, Gartner cited ramped up zero trust implementation as one of the reasons spending on information security and risk management products and services would grow 11.3% in 2023, reaching more than $188.3 billion. The research and consulting firm identified three factors influencing growth in security spending: the increase in remote and hybrid work, the transition from VPNs to zero-trust network access, and the shift to cloud-based delivery models.

"The modern CISO needs to focus on an expanding attack surface created by digital transformation initiatives such as cloud adoption, IT/OT-IoT convergence, remote work, and third-party infrastructure integration," said Ruggero Contu, senior director analyst at Gartner. "Demand for technologies and services such as cloud security, application security, zero-trust network access, and threat intelligence has been rising to tackle new vulnerabilities and risks arising from this exposure."

CRA BI survey respondents agreed, with one saying of the zero-trust component: "There has been a slight learning curve and hurdles to implementing zero trust, but the benefits are worth it."

Endpoint security tested by proliferation of non-traditional devices

The widespread shift to work-at-home environments and the proliferation of non-traditional endpoints had a significant impact on the number of enterprise-related security breaches since 2020.

In 2022 specifically, a multitude of risks emerged to test endpoint security. The explosion of mobile devices continued. Consumers and businesses alike increased their use of the so-called Internet of Things (IoT). And operational technology (OT) that historically was siloed off from the internet saw far more integration with enterprise networks, even among critical infrastructure sectors. The healthcare sector emerged particularly vulnerable, spurring an FBI alert in September 2022 that cited unpatched medical devices operating on outdated software and with a lack of adequate security features.

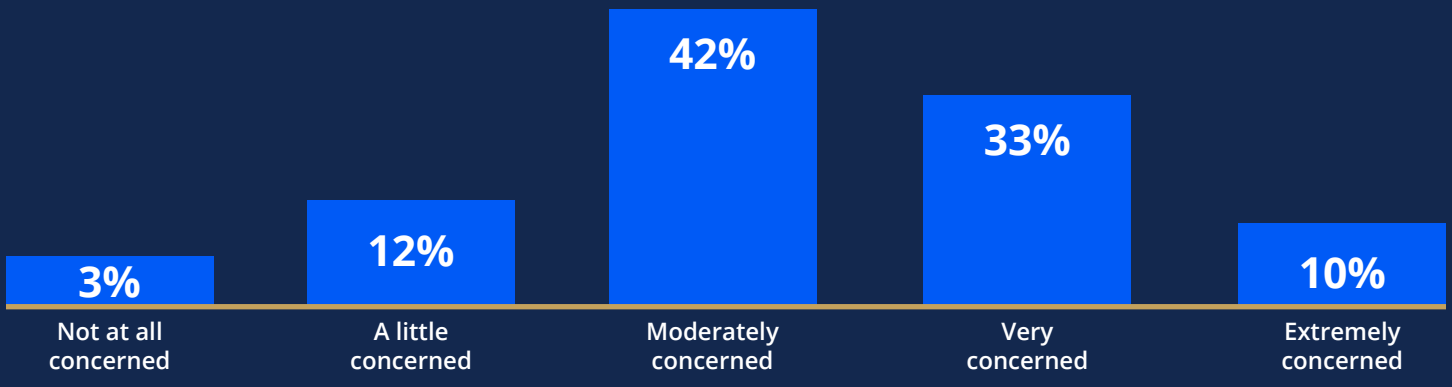
The end result: organizations struggled to obtain a holistic view of all devices and their vulnerabilities, or know how to fix and mitigate them to manage risk and ensure compliance.

Endpoints out of control

To illustrate the endpoint challenges vexing security teams, an EY Consulting study – the results of which were released in an October report – showed that Millennial and Gen Z employees are even more relaxed when it comes to cybersecurity on their work devices than their personal devices. Meanwhile, the risks posed by non-traditional devices were evident in headlines throughout 2022.

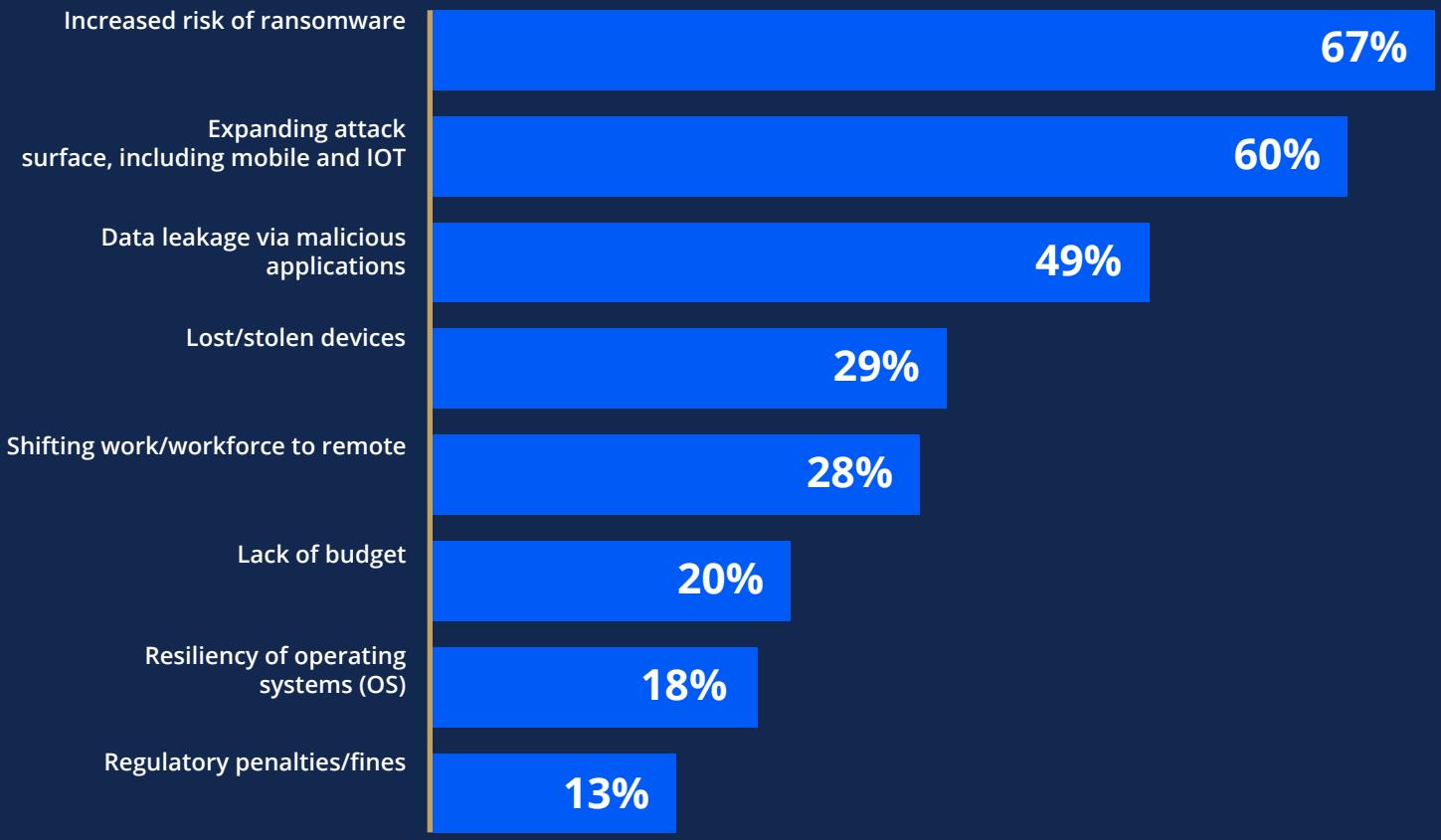
According to an August 2022 CRA BI survey of 204 security and IT leaders and executives, security administrators, and compliance professionals based in the United States, the impact that mobile and other non-traditional endpoints have on security is significant: 43% indicated they are very or extremely concerned about device security in the next 12 months. The fear of ransomware, and the damage it could inflict in their environments, remained a top concern, as reported by about two-thirds of respondents, as did the expanding attack surface and data leakage. Survey respondents cited many challenges to device security, including limited budgets and resources, outdated device policies and compliance, and lack of upper-level management support for device management strategies and purchases.

Overall, how concerned are you about device security over the next 12 months?



CRA Business Intelligence Survey, August 2022.

What are your top three concerns about device security vulnerabilities?



CRA Business Intelligence Survey, August 2022.

According to one respondent, "the most significant hurdles our organization faces in this environment are dealing with the multitude of new mobile devices and OSes being introduced at a faster pace. It makes securing them as endpoints a challenge since the accompanying security solutions tend to lag the introduction of these devices and OSes. This trend will likely only increase in the future, with ever more complex devices being developed."

Push for endpoint security improvements

As the number of endpoints continued to expand, the CRA survey respondents did their best to keep up. In addition to monitoring traditional devices like PCs and servers, a large majority (84%) reported they also monitor mobile devices on their network, with respondents reporting that their security solutions cover large volumes of both traditional and non-traditional endpoints and devices. Nearly two-thirds (63%) of respondents said they are managing more than 1,000 traditional and non-traditional devices.

As vexing a challenge as endpoint security was in 2022, respondents did state that their device security strategies are advancing along with the vulnerabilities and security concerns exacerbated by the remote workforce. Many organizations are evolving their endpoint security strategies to confront their fear of ransomware (61%), building business resiliency (58%) and complying with regulatory requirements (55%).

Many organizations predicted they would increase their budgets to provide better protection. While almost one in four respondents said their device security budgets will remain unchanged in the next 12 months, another 70% indicated they will likely increase their device security budgets at some level. Zero trust and automated remediation were at the top of those spending plans.

Which of the following are currently included – or otherwise planned, or not planned– in your organization's device security strategy?

	Currently Included	Planned	Not planned
Anti-virus/Anti-malware	90%	6%	3%
Patch management	79%	16%	4%
Endpoint detection and response	78%	17%	4%
Vulnerability management	72%	23%	5%
Asset discovery/management	70%	25%	6%
Mobile device security	64%	26%	10%
IoT devices	35%	38%	27%
eXtended detection and response	33%	41%	25%
Zero Trust	31%	52%	17%
Automated remediation	29%	48%	23%
OT/ICS devices	28%	29%	43%

CRA Business Intelligence Survey, August 2022.

As the research suggests, the areas where organizations need the most improvement are around anti-malware, patch management, endpoint detection and response, and vulnerability management. Ransomware, business resiliency concerns, and regulatory compliance mandates will continue to drive spending and strategy to improve device security as they prepare for 2023 and beyond.

Attackers on high ground as organizations struggled to secure email

Security teams devoted much attention to email security in 2022, but attackers continued to have the edge, exploiting the vulnerabilities that come with remote work and the explosion of business and personal devices.

Consider the compromise reported by American Airlines in September 2022. The company informed customers that a bad actor breached the email accounts of some employees in July, which led to the personal information of customers and employees potentially being exposed and accessed.

Also in September, a credential phishing attack targeted 16,000 emails at a nonprofit agency. The fraudster in that incident claimed to be the prominent charge card brand American Express and prompted victims to sign in to verify their account, which of course put cardholders right where scammers wanted them.

Such incidents demonstrate that email security is at its core a people problem, requiring security teams to address risks that can often linger beyond the realm of their control.

The uphill struggle with email security was also captured in a September 2022 CRA BI study among 221 security and IT leaders and executives, security administrators and compliance professionals based in the United States.

Consequences of email insecurity

In the last 2 years, cyberattacks traced back to exploited email vulnerabilities and enabled by users falling for phishing attempts led, in some cases, to uncomfortable consequences.

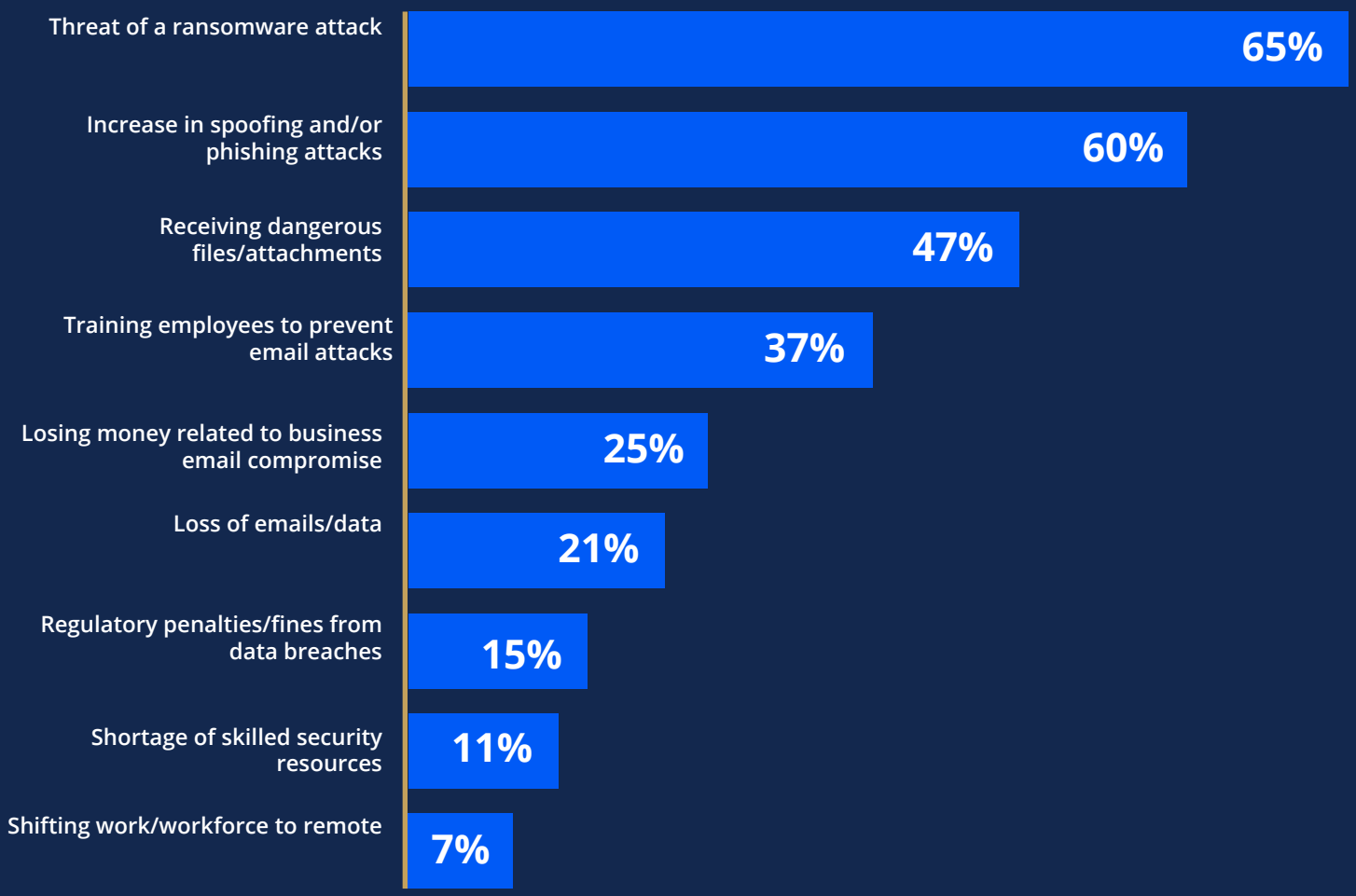
In October, the state of New York slapped EyeMed Vision Care with a fine – not for the first time – over its massive 2020 email hack and healthcare data breach. The vision benefits company was ordered to pay a $4.5 million penalty for multiple security violations that "contributed to" the data exposure. And fallout from that breach for both the company and customers continues.

Indeed, fears of similar fallout from an email security "hack" or "breach" was reflected in results of a May 2022 CyberRisk Alliance (CRA) Business Intelligence study, based on a survey of 221 security and IT leaders and executives, security administrators and compliance professionals based in the United States.

Respondents reported dealing with some form of email attack daily, with attacks on Microsoft and Google email systems rising substantially. That included increased abuse of both Microsoft 365 and Google email infrastructure. In addition to phishing emails designed to capture login credentials, email attacks also contained payloads that included traditional viruses or application macros, such as those that run in Word or Excel.

CRA respondents reported a significant and steady number of email attacks with one-third experiencing up to 25 attacks on a daily basis. Additionally, about half (51%) of all respondents reported up to 25 business email compromise (BEC) attacks per day while one in five (21%) said they didn't know and couldn't estimate the volume of daily BEC attacks. At least half the respondents (51%) said they were very or extremely concerned about email attacks in the next 12 months. The threat of a ransomware attack was a top email security concern for two-thirds of all respondents, followed by an increase in spoofing and phishing.

What are your top three concerns about email security?

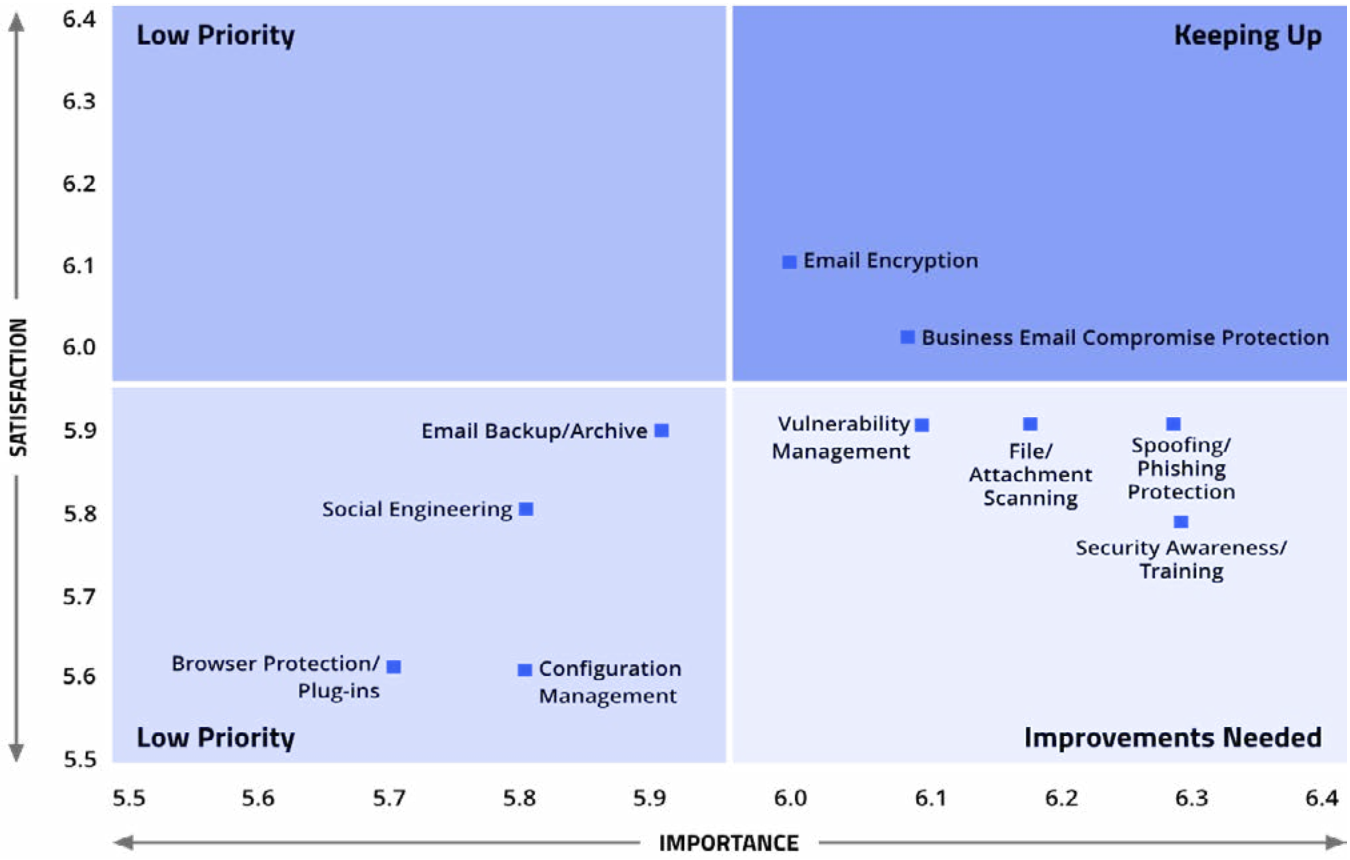


CRA Business Intelligence Survey, May 2022.

"While we do run training sessions and communicate about fraudulent emails, people still click on things they shouldn't, open up emails or attachments when they shouldn't," said one survey respondent. "If they don't get a big red warning from the security systems, they just don't think about every email they touch."

Respondents said they were keeping up with email encryption and business email compromise protection, but were falling behind on vulnerability management, file attachment scanning, phishing protection and security awareness training.

What matters, what's working and what isn't

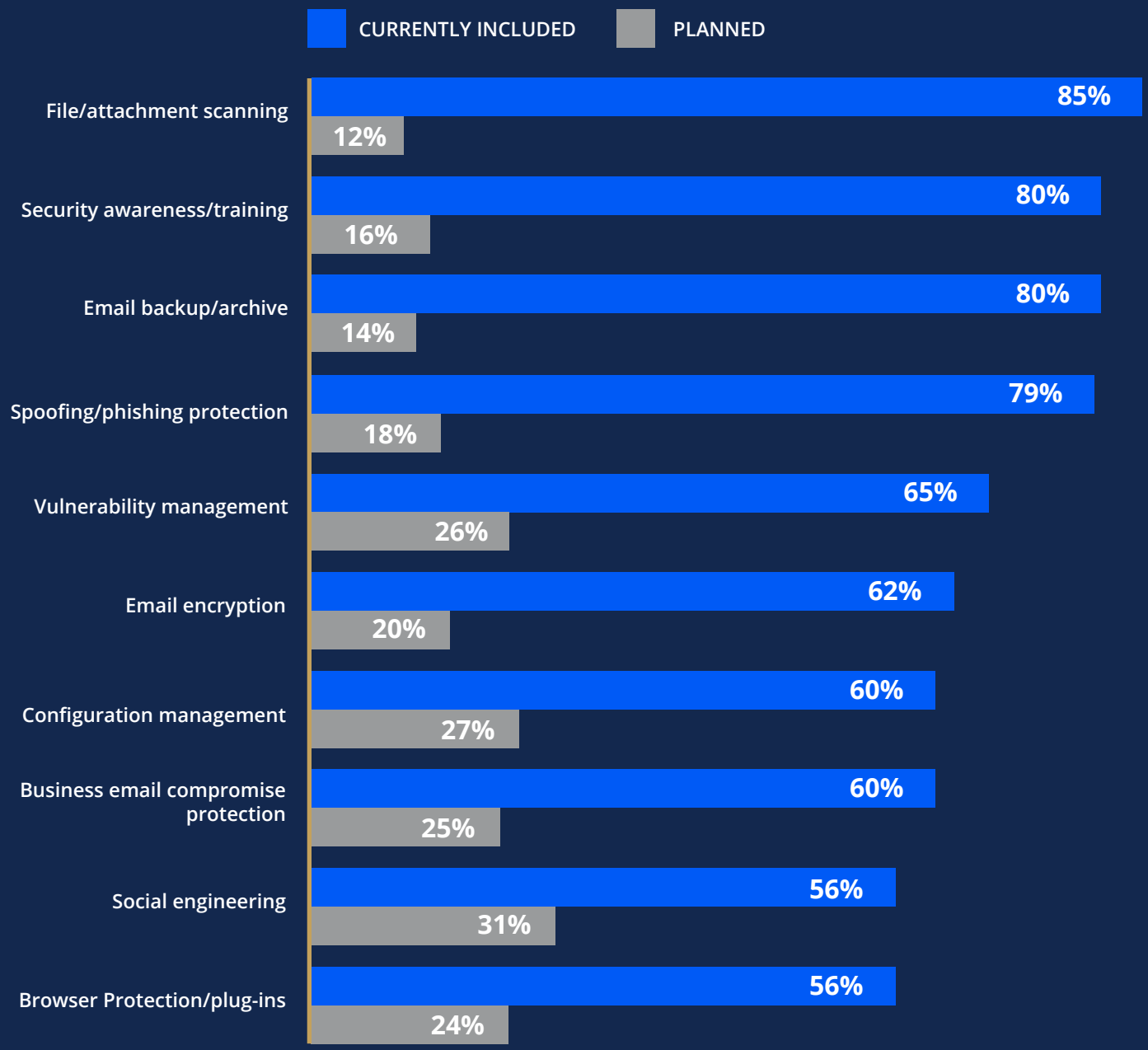


Fighting back with security tech and cyber training

While the email security challenges security practitioners faced were significant, there were some positive developments in 2022, according to the CRA BI survey.

Recognizing the serious risks posed by email attacks, a large share of respondents (68%) reported their organization will likely increase spending on email security in the next 12 months. Education regarding social engineering, configuration management and more BEC protection will grab the majority of those additional dollars.

Which of the following are currently included or planned to be included in your organization's email security strategy?



CRA Business Intelligence Survey, May 2022.

Of course, training is at the heart of plans to address social engineering. Security experts have said the most reliable way to stop email spoofing from succeeding may be by training the workforce to spot bogus emails. No amount of technology can completely stop phishing emails – and no amount of training can either – but a well-educated and well-practiced employee can spot them at least the majority of the time. Combine this stance with DMARC, DKIM and SPF and the odds of a compromise go down astronomically.

Likewise, proper workforce training will educate staffers who manage the company's money about the different tricks used by BEC scammers. (You could also require that more than one employee sign off on large money transfers.) Ideally, employees should participate in dynamic scenarios that simulate common BEC scams.

As one respondent put it, "We need to take a proactive approach to email security solutions as it saves money and time overall. If you are purely reactive, you are wasting valuable time and resources by reacting to an issue."

XDR positioned as force multiplier for threat detection

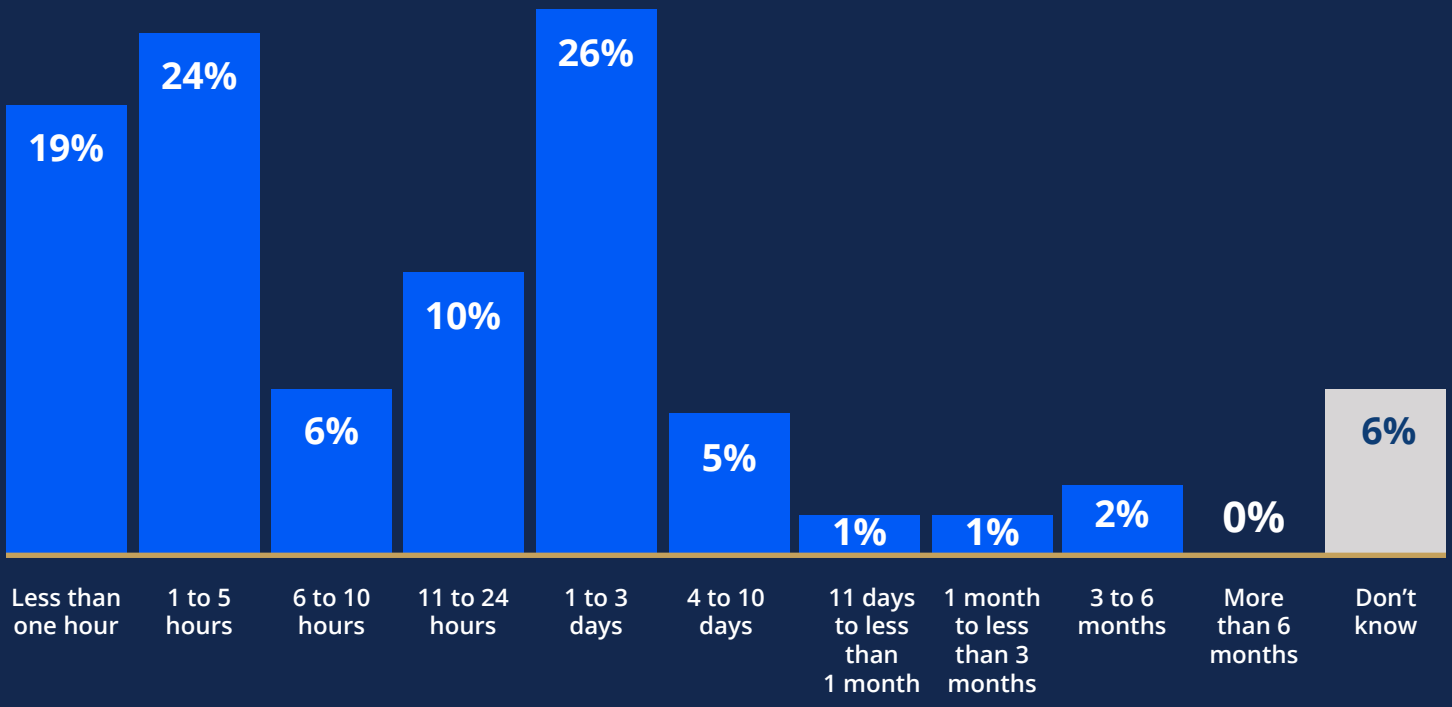
The threat landscape continued to expand throughout 2022 as organizations shifted from on-premises to cloud-based operations and criminal actors exploited the resulting vulnerabilities to flood targets with ransomware and other malware. Along the way, security teams realized that their defensive tools could no longer keep up.

To turn the tide, many security leaders pinned their hopes on eXtended Detection and Response (XDR), albeit by way of observation. Indeed, a March 2022 CRA BI survey of 300 IT and cybersecurity decision-makers and influencers from the United States found that while current XDR adoption levels were low, interest was high.

The interest in XDR, which essentially takes a more holistic approach to threat protection, reflects concerns among security leaders that the sophistication of attacks, more often than ever before, leads to failure in detection. One respondent pointed to a data breach last year that the organization didn't detect until the damage was done.

"We didn't see any red flags; everything was normal," the respondent said. "However, we were actually under attack. Even though we discovered it in less than 10 days, that's still a lot of time when you're under attack. I know some companies don't find out that they suffered a data breach after like six months, and that's really crazy."

To the best of your knowledge, what is the average estimated time it typically takes to detect and identify real cyberthreats at your organization?



CRA Business Intelligence Survey, March 2022.

The need for more advanced security tools

Security vendors, seeing the growing hunger for next-generation solutions, moved to enhance their XDR portfolios throughout 2022.

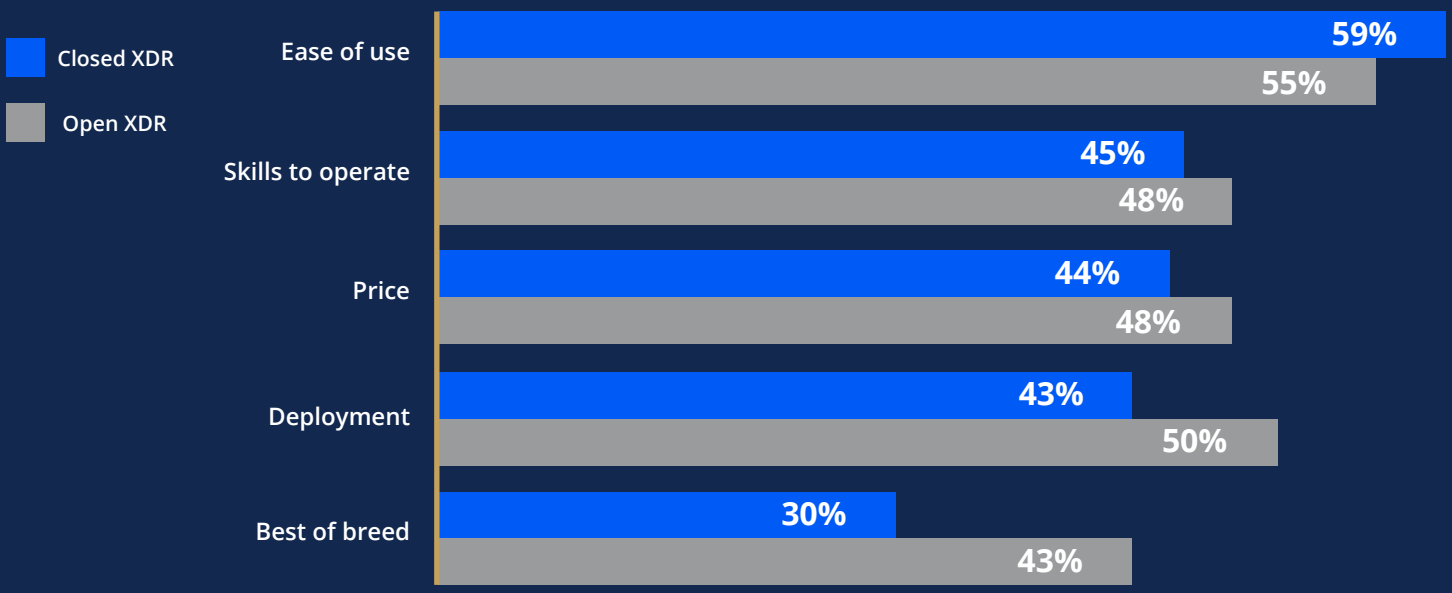
During CrowdStrike's Fal.Con 2022 event in September, for example, the company unveiled updates to its various security products and an expansion of its CrowdXDR Alliance. Crowdstrike announced the joining of Cisco, Fortinet, and ForgeRock to the CrowdXDR Alliance and revealed plans to integrate telemetry with its third-party partner vendors.

Elsewhere, Armorblox announced the integration of its cloud-based email security platform with SentinelOne Singularity XDR to protect businesses against socially engineered targeted attacks. The two companies said tight integration between XDR and email security will let security operations (SecOps) teams deepen threat investigations and accelerate responses to business email compromise, financial fraud, and sensitive data loss.

The frustration of security practitioners with current security tools was evident in CRA BI's survey responses. For example, the lack of visibility or context from existing security solutions caused 47% of respondents to miss threats at least once in the past 12 months. Only 17% said they were very satisfied with their ability to correlate security data across all products and services.

Without the ability to see anomalies and/or malicious activities as they occur and across the spectrum of products and services, it's impossible to catch everything. Poor visibility into network threats was seen as a significant problem for monitoring employee-owned endpoints, software vendors and third-party partners.

In considering an XDR technology investment, which of the following do you think are the top benefits of an open XDR infrastructure (which integrates with existing security tools) vs. a closed (single vendor) XDR-ready infrastructure?



CRA Business Intelligence Survey, March 2022.

Security teams integrating XDR into future plans

While familiarity with XDR is high (70%), current adoption of an XDR platform is relatively low; only 12% of respondents reported using this technology. But for those either using the technology or planning to invest in it, top benefits include faster detection and overall risk management improvement.

While XDR technology has yet to become widespread, a large majority (77%) of respondents said they are somewhat or very likely to invest in XDR technology in the next two years.

“It runs smoothly with other software we are using and catches almost every threat and issue,” said one current user who took the survey. “It is easy to deploy, easy to update, can make changes as needed quickly, and our employees are able to get up to speed quickly.”

Vulnerability management strategies grow more aggressive and proactive

Vulnerability management remained a thorn in the side of security teams in 2022. As organizations continued moving to cloud-based operations and grew increasingly dependent on third-party partners, fresh software security holes materialized at a rate that was impossible to match, whether it be zero-day vulnerabilities in Microsoft Exchange or a dangerous cloud isolation vulnerability in Oracle Cloud Infrastructure (OCI).

But security teams were undeterred, investing in more aggressive, proactive vulnerability management strategies, according to a July 2022 CRA BI survey of 213 security practitioners. The survey showed organizations embracing continuous security assessments and automated remediation processes to stay ahead of newfound flaws and attacker exploits.

"We are more vulnerable due to more of our staff working remotely and accessing our information in different environments," said one respondent. "This is the main reason why we have changed our vulnerability strategy."

Ongoing vulnerability management challenges

For security teams, the biggest obstacle to vulnerability management continued to be the sheer number of security holes to track. In one example from October, Microsoft updated the mitigation measures security teams should undertake for recently disclosed Exchange vulnerabilities that could lead to remote code execution after it was reported that previous measures were easily bypassed.

Then there was the revelation in October that a vulnerability in the Citrix Application Delivery Management (ADM), believed to have been patched in June, was not sufficient to prevent exploitation.

Meanwhile, in September, IBM Security X-Force reported that amid a sixfold increase in new cloud vulnerabilities over the past six years, 26% of cloud compromises that X-Force responded to were caused by attackers exploiting unpatched vulnerabilities.

Claude Mandy, chief evangelist of data security for Symmetry Systems, said, at the time, that organizations must prioritize which vulnerabilities get patched first, not only find them.

"Prioritization of vulnerabilities should consider a number of factors, including the severity, existence of public exploits, and accessibility of the vulnerability and the business criticality and sensitivity of the asset and data at risk," Mandy said. "In the cloud, the complexity and scale quickly becomes unmanageable without use of vulnerability prioritization technology."

CRA survey respondents revealed many challenges in implementing and enhancing their vulnerability management programs: budget, endless patching, and proliferation of tools, to name a few.

Challenges in implementing vulnerability management*

(% of respondents mentioning each area)

30%
Budget or Resources

"Budget is the hardest justification. RPO/RTO is currently not quantified so it's hard to recognize impacts to the business."

"Dealing with the high volume of vulnerabilities found, particularly in vendor supplied systems. Getting vendors to remediate at an acceptable speed is a challenge.

18%
Patching or remediation

14%
Tools and products

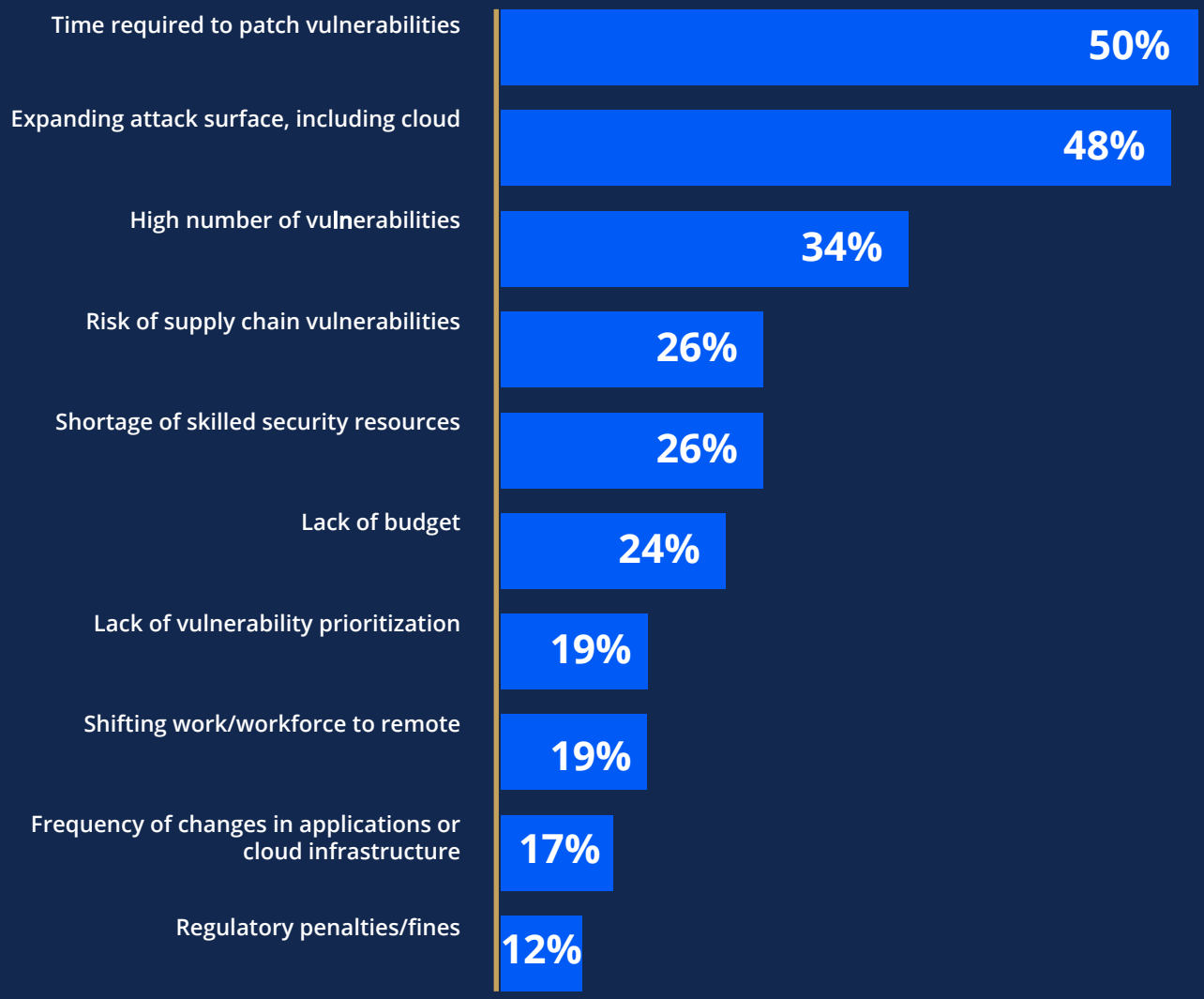
"The use of different tools to cover what other tools lack."

"Wide variety of assets deployed in on prem, cloud and remote networks."

8%
Assets or scanning

*What are your organization's challenges or issues in effectively using vulnerability management to reduce the risks to your business-critical assets?

What are your top three concerns about vulnerabilities?



CRA Business Intelligence Survey, July 2022.

Efforts to turn the vulnerability tide

In the face of those hurdles, security practitioners doubled down on more aggressive vulnerability management strategies in 2022. Those who implemented more robust vulnerability management programs harnessed a combination of enhanced toolsets and automated solutions, increased scanning, expanded coverage of assets, improved patch management, and continuous vulnerability monitoring.

Respondents spoke out about their top vulnerability management challenges and changes they've made since 2020, which focused on the integration of new tools and technologies and adapting procedures to keep up with the evolving threat environment.

Additionally, some CRA survey respondents underscored their focus on vulnerability prioritization to address the more exploitable vulnerabilities of their higher-value assets. And in many instances, increased budgets, resources, and staff allocations were put in place to bolster security programs. More than two-thirds, (69%) of respondents, said their budget or spending on vulnerability management would increase in the next 12 months, especially for things like automation:

Which of the following are currently included, or planned to be included, in your organization's vulnerability management strategy?

	Currently Included	Planned	Not planned
Patch management	75%	18%	7%
Asset discovery/management	67%	25%	8%
Continuous monitoring	66%	24%	10%
Configuration management	63%	27%	10%
Customizable reporting	55%	28%	17%
Vulnerability prioritization	52%	37%	11%
Attack path analysis/visualization	40%	34%	25%
Custom risk scoring	38%	33%	30%
OT/ICS vulnerabilities	32%	36%	32%
Automated remediation	26%	46%	29%

Respondents spoke out on their top vulnerability management challenges and changes they've made since 2020, which focused on the integration of new tools and technologies and adapting procedures to keep up with the evolving threat environment.

Said one respondent: "Since COVID, our budget increased considerably, and new strategies were implemented. The problem now is to keep the budget."

Changes in vulnerability management strategy since 2020*

(% of respondents mentioning each area)

13%
Increased tools or automation

"Increased use and reliance on AI/ML, automation, modeling and calculated risks."

"We have invested a considerable amount of money towards proactive scanning and remediation of both external and internal attacks."

13%
More frequent or additional scanning

12%
Focused on remote workforce

"Focus more at the endpoint level due to remote workers."

"Since COVID, our budget increased considerably, and new strategies were implemented. The problem now is to keep the budget."

9%
Increased resources (Staff or investments)

*What are your organization's challenges or issues in effectively using vulnerability management to reduce the risks to your business-critical assets?

New threat intelligence tools help secure systems – and educate executives

Amid the heightened fear of ransomware in 2022, threat intelligence emerged as a core requirement of doing business in a world gone mad.

A sizable amount of interest in the historically tech-centric discipline was fueled in part by fear of cyberattacks tied to the war between Russia and Ukraine. In one example, the Ukrainian government warned the world that the Russian military was planning for multi-pronged attacks targeting the energy sector. Other nation-state cyberattack operations also contributed to the demand, including one June 2022 incident where Iran's Cobalt Mirage exploited PowerShell vulnerabilities to launch ransomware attacks.

And of course, headlines of data breaches tied to vulnerabilities that organizations did not even know existed within their networks caught the attention, not just of security teams, but the C-Suite and corporate board. A misconfigured Microsoft server, for example, wound up exposing years of sensitive data for tens of thousands of its customers, including personally identifiable information, user data, product and project details and intellectual property.

Indeed, according to 183 security pros surveyed by CRA BI in June 2022, threat intelligence has become critical in arming their security operations centers (SOCs) and incident response teams with operational data to help them make timely, informed decisions to prevent system downtime, thwart the theft of confidential data, and protect intellectual property.

Threat intelligence used to educate execs

Threat intelligence has emerged as a useful tool for educating executives. Many also credited threat intelligence for helping them protect their company and customer data — and potentially saving their organization's reputation.

"Without threat intelligence you would be chasing ghosts," said one CRA survey respondent.

Respondents reported their top use cases for threat intelligence are vulnerability management (68%), security operations (66%), and incident response (62%). Technical (73%) and operational (71%) threat intelligence are more common than the more difficult strategic or more basic tactical use cases. Only 5% said they did not use any threat intelligence.

Many respondents pointed out that having access to early and credible intelligence is a core requirement for their organization. About six in 10 participants said they had subscribed to up to 10 threat intelligence feeds, while another quarter gathered their intelligence from 11 to 50 feeds. The largest share of respondents was using threat data from malware analyses or indicators of compromise (IOC).

Challenges of threat intelligence

Effective implementation of threat intelligence isn't without its challenges. Companies face everything, from internal obstacles and competing priorities, such as limited resources and lack of skills/qualified staff, and budgeting/financial constraints, to issues related to dealing with the evolving threat landscape and expanding attack surface.

Unfortunately, the ability to implement automated security responses to threats, enabling detection and remediation of the latest types of attacks, remains out of reach for many. Some claim actionable intelligence is hard to find, while others grapple with threat data overload and collating and assembling critical attack data, along with controlling excessive alerts and false positives.

Finding the most efficient solution that enables rapid deployment and the greatest ROI was also considered problematic, as well as intelligence integration and the deployment of advanced technologies, such as machine learning models that optimize the use of historical data to predict future events.

Threat intelligence investments planned

Given the need for more threat intelligence, survey respondents were planning to Increase their investments, with 66% expecting their organizations to invest more in the coming year. Automation and threat modeling are especially sought after by security teams, based on planned investments.

Top challenges in effectively using threat intelligence*

(% of respondents mentioning each area)

33% Resources and skills

"Finding the correct people and building processes to help make this effective."

"I think it's the vast amount of threats that have escalated in the past 3 to 6 months and also keeping up with the massive amount of patching."

30% Changing threat landscape

20% Budget and funding

"Budget is always a hot topic and never really gets better. Trying to get the organization to be adaptable to new threats and to be prepared is always challenging."

"...full visibility into the ICS environment. Many of the current tools are not designed to work or integrate with these types of devices. The age of this equipment does not allow for integration or agent type installs, so upgrades to those systems are needed."

19% Tools and integration

19% Data and intelligence

"Assessing the relevance of the intelligence to our type of organization. Much of it is centered on government, defense, or other large corporate targets rather than the smaller organizations. We have a different threat profile."

*What are your organization's challenges or issues in effectively using vulnerability management to reduce the risks to your business-critical assets?

This specific trend bodes well for security operations centers hoping to boost defense capabilities through improved threat intelligence, particularly as it relates to patching security flaws in current software and responding more quickly to security events.

Which of the following are currently included or planned to be included in your organization's threat intelligence strategy?

	Currently Included	Planned	Not planned
Data integration (SIEM, EDR, FW, etc.)	59%	28%	13%
Information sharing	52%	32%	15%
Threat intelligence platform	50%	28%	22%
Automated action/response	46%	41%	13%
Internal vs. external threat comparison	45%	37%	19%
Threat modeling	34%	37%	29%
Mitre att&ck framework	33%	28%	38%
Statistical data analysis	33%	35%	32%
Machine learning	30%	35%	36%
Cyber kill chain methodology	24%	27%	49%

One respondent said her own organization's plans to spend more on threat intelligence was critical to understanding exactly how systems are being attacked and building a plan to detect and respond.

As she put it: "Knowledge is everything."

About RSAConference™

RSA Conference is the premier series of global events and year-round learning for the cybersecurity community. RSAC is where the security industry converges to discuss current and future concerns and have access to the experts, unbiased content and ideas that help enable individuals and companies to advance their cybersecurity posture and build stronger and smarter teams. Both in-person and online, RSAC brings the cybersecurity industry together and empowers the collective "we" to stand against cyberthreats around the world. RSAC is the ultimate marketplace for the latest technologies and hands-on educational opportunities that help industry professionals discover how to make their companies more secure while showcasing the most enterprising, influential, and thought-provoking thinkers and leaders in cybersecurity today. For the most up-to-date news pertaining to the cybersecurity industry visit www.rsaconference.com. Where the world talks security.

About CyberRisk ALLIANCE

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, and now, the Official Cyber Security Summit and TECHEXPO Top Secret. Click here to learn more.

INTRODUCING THE **RSAC CISO PERSPECTIVES SERIES**

For CISOs—or any cybersecurity professional—RSA Conference provides year-round insights and resources to help better secure your organization. Now available, our first CISO Perspectives report.

The first report in our series discusses **What Top CISOs Include in Updates for the Board**. The RSAC Executive Security Action Forum (ESAF) Program Committee tapped into the world's foremost enterprise security leaders from seven industries to create this comprehensive report examining what vital information CISOs share when addressing the board.

Download the report at RSAConference.com/CISOreport, then be on the lookout for the next report in our CISO Perspectives series.

Discover Why We Are **Stronger Together**

Join us at RSAC 2023, April 24 – 27, in San Francisco for four days of eye-opening Keynotes, informative sessions, and opportunities to connect with experts and peers.

Learn more at RSAConference.com/usa!