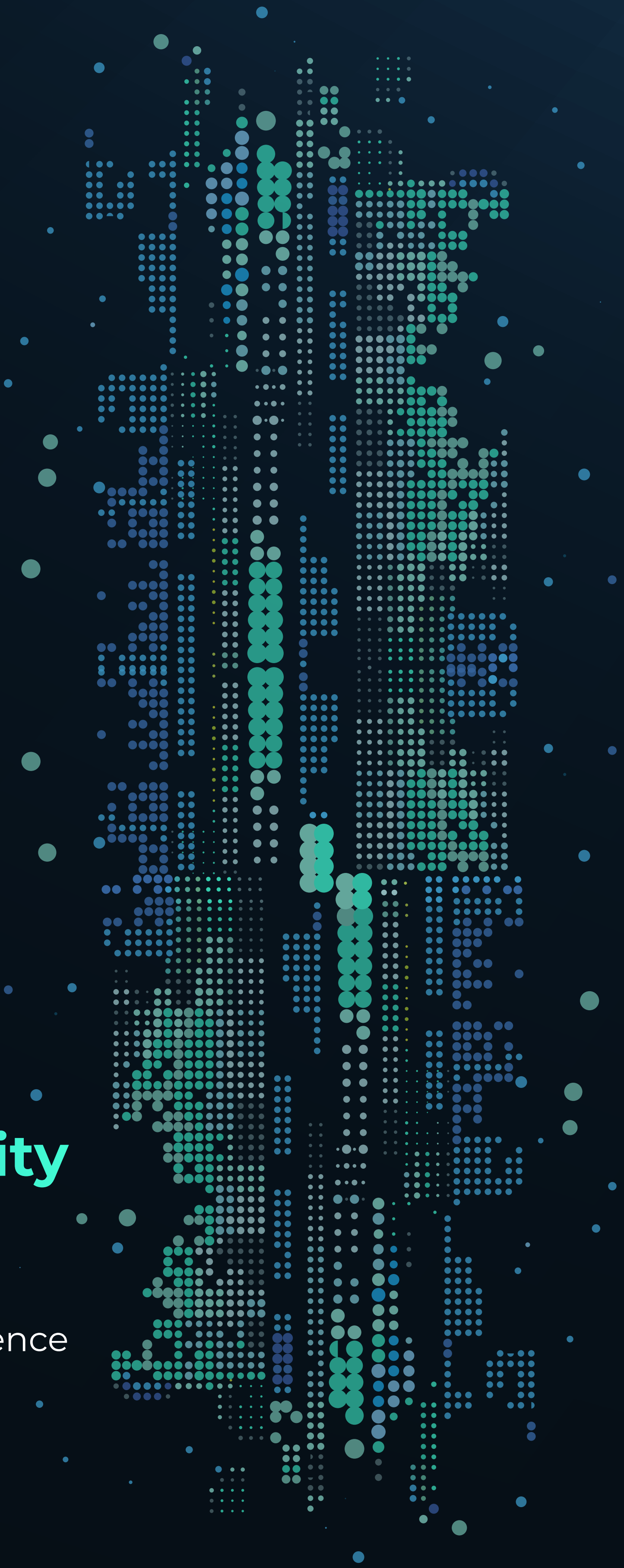
ANOMALI



2022

Anomali Cybersecurity Insights Report

The State of Enterprise Cyber Resilience

Table Of Contents

PAGE

Introduction

Welcome to the *Anomali Cybersecurity Insights Report 2022*. In this inaugural research, we identify the challenges enterprises face in establishing and maintaining resilient cybersecurity postures and explore what is needed to protect and respond to the advanced cyberthreats of today and tomorrow.

To gather and develop foundational data for this report, the Anomali Threat Research team commissioned The Harris Poll to survey 800 Security Decision Makers across 11 countries from enterprises with 5,000 or more employees. Because COVID-19 has had such a profound impact on business and cybersecurity, we queried these decision makers to understand their cybersecurity postures and challenges going back to 2019, to provide a better understanding of how the global pandemic has affected businesses. Threat intelligence analysts from the Anomali Threat Research team reinforced the findings with threat trend analysis, giving readers actionable information they can use to improve their ability to detect and respond to breaches and attackers.

Among the top takeaways is that even with significant investments made in cybersecurity, **many organizations face obstacles to achieving the level of cyber resilience needed to protect against, detect, and respond to attackers**. This finding likely comes as no surprise to most readers, given the increase in breaches and cyberattacks the world has been experiencing over the past several years.

CYBER RESILIENCE DEFINED

The ability to proactively and reactively protect your organization against threats and attackers, adapt to changing circumstances during an attack, and recover after a cyberattack has occurred.

Executive Summary

Our research uncovered many reasons why achieving cyber resilience is difficult. At the top of the list, organizations struggle with performance and capability gaps in the level of detection, response, and recovery needed to address immediate and future attacks and breaches.

This research revealed that cyberattacks are increasing (up **15%** from 2019 pre-pandemic levels). It therefore came as no surprise to us that around three out of four (**74%**) organizations have increased their cybersecurity budgets and are re-evaluating their cybersecurity strategies (**78%**).

Even with increased investment, most businesses (**87%**) have fallen victim to successful cyberattacks in the past three years that resulted in damage, disruption, or a breach to their businesses. Despite their efforts, around two-thirds (**67%**) say more successful cyberattacks have impacted their organization since the start of the pandemic. In 2020 alone, one in seven (**14%**) cyberattacks on average were successful, resulting in a breach, damage, or operational disruption. Security Decision Makers expect this number to climb, as their attack surfaces are expanding alongside the unprecedented scale of digital transformation projects. Even with this increasingly dangerous threat landscape, only 44 percent have identified incident response best practices they can employ when attacked.

87%

Of enterprise Security Decision Makers say their organization has experienced a successful cyberattack attack in the past three years that resulted in damage, disruption, or a breach to their business.

Cyber incidents are taking a financial toll on nearly all organizations, with losses from targeted cyberattacks, malware campaigns, phishing, insider threats, and associated data breaches running well into the hundreds of thousands of dollars per organization. Nearly three in 10 (**28%**) businesses globally reported losses of $500,000 or more in 2020, up nearly two-fold (**193%**) from 2019 and nearly half (**47%**) reported losses of $100,000 or more. In addition to significant losses, the attacks themselves are increasing at an astounding rate.

In addition to factors such as the rapid pace of digital transformation and rising attacks, many Enterprise Security Decision Makers cited a lack of integrated cybersecurity solutions as a barrier to detecting, responding to, and recovering from cyberattacks and data breaches.

Many respondents say their organizations have started using, or are planning to invest in, recent technology innovations associated with Extended Detection and Response (XDR) and Advanced Threat Intelligence to counterbalance obstacles.

What is clear is that there is an appetite for cybersecurity solutions that are well supported (**48%**), easy to use (**46%**), and better integrated into existing frameworks and architectures (**44%**), with more than four in 10 decision makers considering these attributes to be essential.

TOP CHALLENGES TO ACHIEVING CYBER RESILIENCE

Finding 1

Organizations are Only Moderately Effective at Detecting, Responding to, and Recovering from Cyberthreats

Forty-two percent of Security Decision Makers believe they have not achieved the level of resilience needed to defend their organizations against breaches and attacks. Fewer than 6 in 10 (58%) decision makers strongly agree their organizations are cyber resilient, however, this finding contrasts with the fact that 87 percent of organizations have been breached over the past three years.

Finding 2

Just Under Half of Security Decision Makers Strongly Agree that Their Cybersecurity Teams Can Quickly Prioritize Threats Based on Trends, Severity, and Potential Impact

One-third admit that their teams struggle to update security controls to address new attacks (31%). Less than half (49%) of Enterprise Security Decision Makers strongly agree that their cybersecurity teams can quickly prioritize threats based on trends, severity, and potential impact. Even fewer (46%) are very confident that their cyber-protection technologies can evolve to detect new globally identified threats. One-third (32%) admit that their teams struggle to keep up with the changing cybersecurity threat landscape. Smaller organizations are even more at risk. Those with fewer than 10,000 employees are less apt to be armed with a set of best practices they can reference to respond to cyberattacks (40%).

Figure 1.0

ORGANIZATIONS CYBER RESILIENCY (% STRONGLY AGREE)

49%

STRONGLY AGREE

My team can quickly prioritize threats based on trends, severity and potential impact on our organization

46%

STRONGLY AGREE

My cybersecurity technologies can evolve to detect new globally identified threats

32%

STRONGLY AGREE

My team struggles keeping up with the rapidly changing cybersecurity threat landscape

Finding 3

Organizations Fall Short on Goals in Detecting and Responding to Cyberthreats

Dwell Time is the period between when an adversary gains access to a network, is detected, and then stopped. Dwell Time is directly proportional to the amount of damage an attacker can cause. The longer they are inside your network, the more insights gained, the more data and IP stolen, and the more systems they can move into and infect with ransomware and other threats. It is estimated that attackers can evade detection for as long as 140 days, on average. But this metric is specific to the first time a threat is detected and then disclosed.

Another aspect of Dwell Time that is equally precarious is the amount of time it takes to determine whether a newly disclosed threat is also present in your environment. As part of the survey, we asked organizations how long it took to detect and respond to attacks that had been disclosed previously. The results were alarming, as on average all Security Decision Makers admitted that they are not meeting their detection and response goals overall and are also lagging when it comes to specific threat types.

Figure 1.1
MEAN TIME TO DETECT & RESPOND VS GOAL
(in days)

	Data Breach		Network Compromise		Cyberattack	
	Mean Time	Avg. Goal	Mean Time	Avg. Goal	Mean Time	Avg. Goal
DETECT	3.1	2.1	2.8	2.1	2.7	2.5
RESPOND	2.5	2.2	2.5	2.1	2.4	2.1

Effective security operations teams will pay close attention to both their MTTR and MTTD metrics when it comes to solving incidents. It's crucial to be fanatic about reducing these metrics inside organizations, as shorter Dwell Times reduces the overall risk of damage and disruption. Reducing Dwell Times (MTTD and MTTR) begins with understanding attacks and their impact. Organizations also need to break down silos and collaborate cross-functionally to ensure effective detection and response processes.

MTTD

Mean time to detect, or MTTD, reflects the amount of time it takes your team to discover a potential

MTTR

Mean time to respond, or MTTR, is the time it takes to control, remediate and/or eradicate a threat after it's been discovered.

Figure 1.2
MEAN DAYS TO DETECT KNOWN CYBERATTACKS

3.6	3.5
Cybercriminal Organizations	Individual Hackers
3.3	2.9
APTs	Nation State

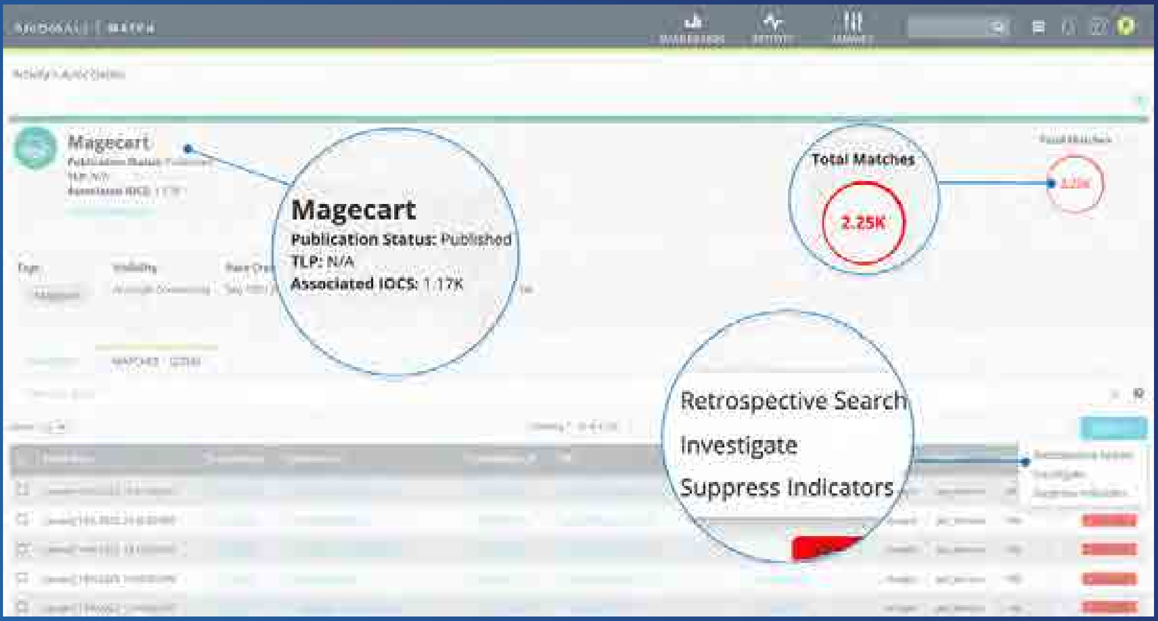
Figure 1.3
MEAN DAYS TO RESPOND & RECOVER FROM CYBERATTACKS

● RESPOND ● RECOVER

	RESPOND	RECOVER
SolarWinds Breach	2.9	3.1
Supply Chain Attack	2.8	3.4
Ransomware	2.4	2.8

Anatomy of Threat Detection

MAGECART: a malicious cybercriminal group targeting e-commerce websites to steal payment card information to sell on criminal forums.



Magecart
Publication Status: Published
TLP: N/A
Associated IOCS: 1.17K

There are many different threat types, and detecting them is typically just one aspect of the mitigation and response. Gathering more information is crucial in making data-driven decisions about threats.

Cybersecurity professionals are now using big data analytics to identify threats before they happen. With the right technologies, this data can be analyzed to gain insights into human behavior, predict future trends, or prevent security breaches.

The example above shows how tools that integrate vast amounts of big data, including indicators of compromise (IOCs), observed behaviors, adversary knowledge, and threat models can be used by analysts to know immediately if threats like Magecart are present in their environments and how long they've been present. When organizations have access to such immediate intelligence, they can respond quickly and decisively, which is critical to setting up a proactive and resilient security posture.

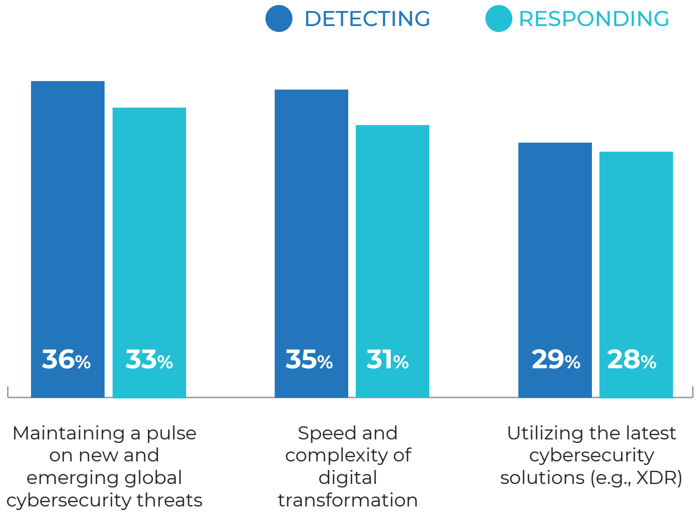
Finding 4

Maintaining a Pulse on New and Emerging Global Cybersecurity Threats, and Speed and Complexity of Digital Transformation are Top Challenges

Organizations face many challenges when it comes to detection. Among the top are keeping a pulse on new and emerging global cybersecurity threats (36%), speed and complexity of digital transformation (35%), and adoption of cybersecurity advancements such as XDR (29%). Nearly identical challenges were noted for responding to and recovering from threats.

Figure 1.4

CHALLENGES WITH CYBERATTACKS, NETWORK COMPROMISES & DATA BREACHES



Finding 5

The Lack of Ability to Share Threat Intelligence Across Internal Resources is Hampering Mitigation Efforts

Maintaining a pulse on new and emerging global cybersecurity threats and the speed and complexity of digital transformation are among the challenges cited by Enterprise Security Decision Makers. But more than anything else, it may be the lack of integrated solutions and the ability to share threat intelligence cross-functionally that most hampers efforts to detect, respond to, and recover from cyberattacks. Slightly more than half (53%) of decision makers feel their organizations are very effective at sharing threat intelligence information across internal resources.

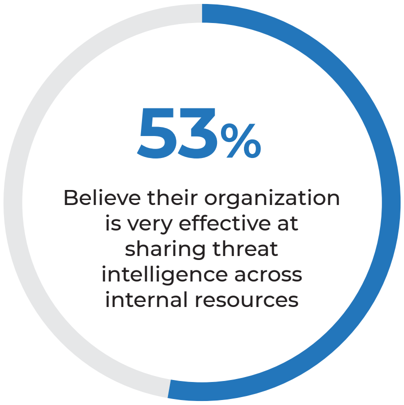
TOP CHALLENGES TO ACHIEVING CYBER RESILIENCE

Threat intelligence is complex and variables are numerous and often described differently. For information sharing efforts to be successful, standards such as MITRE, NIST, STIXX, and others have emerged, which have improved processes.

To understand how to share, organizations must also know what they are attempting to distribute. To further reduce complexity, threat intel can be broken down into two categories, IOCs and Threat Actors, which can help security and risk professionals to understand how to use it.

Figure 1.5

EFFECTIVENESS OF SHARING THREAT INTELLIGENCE ACROSS INTERNAL RESOURCES



IOCs

- OSINT (open source intelligence) feeds can be easy-wins if processes are in place to digest and label data accordingly.
- Threat Intelligence Platforms (TIPs) can do a lot of this work for you by amalgamating threat intel feeds from your intel sources (both free and commercial).
- IOC databases and repositories like AlienVault (OTX), Hybrid Analysis, MalwareBazaar, PolySwarm, VirusTotal, VirusBay, VirSCAN, URLhaus, and URLScan, among others, are excellent tools for gathering context and making data-driven decisions.
- Sandboxes like AnyRun, Hatching, Hybrid Analysis, Inquest, Joe, and Valkyrie Comodo, among others, are helpful to see overall trends and TTPs to create signatures for common malware tactics.
- OSINT detection language repositories for Yara, SIGMA, Snort, and others, are a great way to cover common malicious behaviors.

THREAT ACTORS

- OSINT sources like ThaiCERT, MITRE Groups, Malpedia, and Maltego are excellent sources of threat data.
- TIPs should have many threat actors documented and IOC associations in real-time to keep updated on prolific groups.
- Knowing which malware families are run by different groups, sold “as a service,” modified commodity malware, legitimate tools, or custom malware, will allow a proactive stance when building mitigations for these threats.

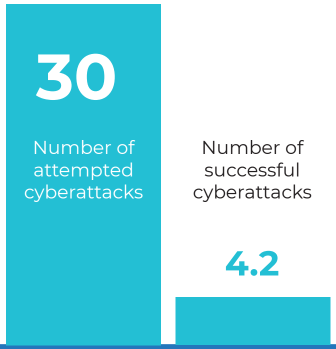
Categorizing intelligence types helps make it more actionable to detect and respond to attackers and breaches. Organizations are turning to innovations that help automate and operationalize threat intelligence across security infrastructures to optimize its value further. Recent reports issued by top industry analysts reveal that demand for solutions in the threat intelligence market, which includes threat management platforms, will spike by as much as 16 percent annually over the next three years.

Finding 6

Cyber Incidents are Widespread and Have Increased Since the Start of the Pandemic

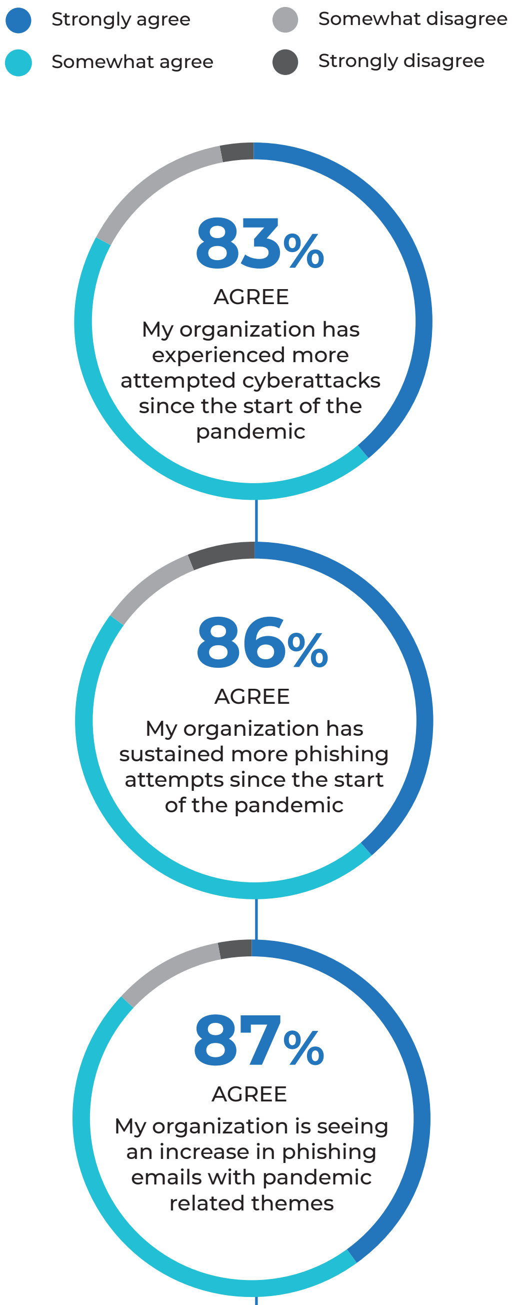
Most Enterprise Security Decision Makers agree that their organizations have experienced more attempted cyberattacks (83%) and sustained more phishing attempts (86%) since the start of the pandemic. Notably, these organizations are also experiencing increased phishing emails with pandemic-related themes (87%). In 2020, businesses with 5,000 or more employees reported 30 cyberattacks on average, up from 26 only one year earlier. One in seven of these cyberattacks (14%) were successful, resulting in damage, disruption or a breach to networks, infrastructure, and devices.

Figure 2.2
MEAN AMOUNT OF CYBERATTACKS ON ORGANIZATION



Organizations with 10,000 or more employees sustained more attempted cyberattacks in both 2019 and 2020 compared to organizations with 5,000-9,999 employees (In 2019, 29.1 vs. 23.3; In 2020, 32.4 vs. 27.8)

Figure 2.1
UPTICKS IN TYPES OF CYBERATTACKS SINCE THE PANDEMIC

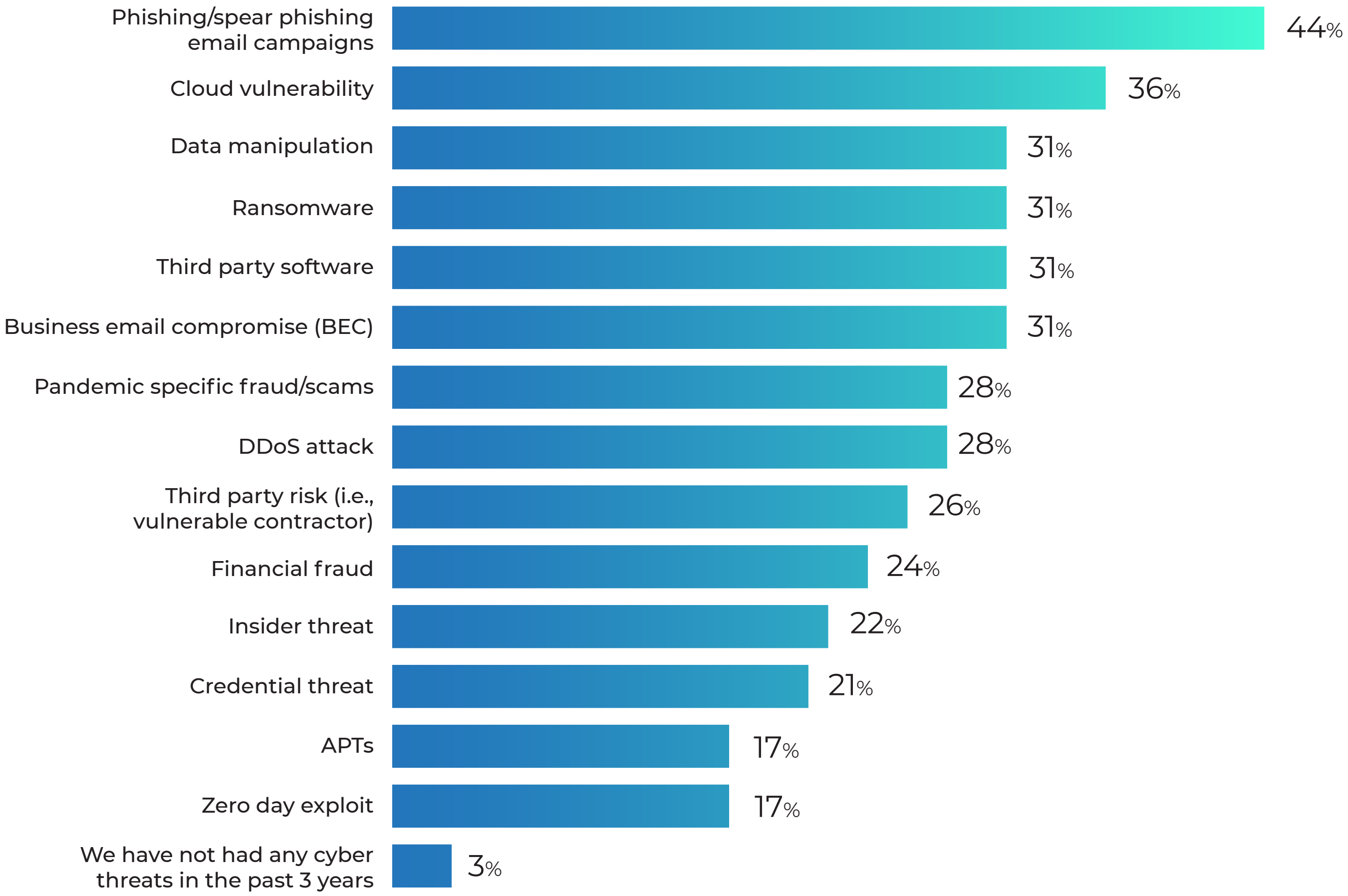


Finding 7

Phishing Email Attempts Are the Threat Encountered Most Frequently

Forty-four percent of all organizations sustained phishing attacks in the past three years, the most common attack experienced. Threat actors of all sophistication use phishing due to available commodity tools and the always-growing target pool. Commodity phishing kits allow low-sophistication threat actors to conduct potentially damaging campaigns that deliver commodity malware. The malicious documents (maldocs) themselves are also commoditized through tools like **EtterSilent**. Threat actors and groups also compromise target email accounts to propagate malicious activity further. They often include legitimate documents to make their activity appear more authentic. Our research has observed the use of legitimate documents in campaigns by **Gamaredon** (Primitive Bear) and **Mustang Panda**, with the former likely using private documents before they are published.

Figure 2.3
CYBER THREATS EXPERIENCED IN PAST 3 YEARS



Finding 8

Cybercriminal Organizations are Perceived to be the Greatest Threat to Cybersecurity (44%), Followed by Individual Hackers (21%)

It Takes 3-4 Days on Average for Businesses to Detect Attacks from these Entities Following Disclosure

Forty-four percent of Enterprise Security Decision Makers say cybercriminal groups are the greatest threat to their organizations. We didn't perceive this as a surprise, as the most damaging attacks and breaches occurring today result from this threat actor type. Fifteen percent of Enterprise Security Decision Makers believe that actors backed by nation states pose the most significant cybersecurity threat to their organizations, with Russia (39%) and China (33%) topping the list. Fewer are concerned about threats emanating from Iran (10%) or North Korea (8%). Security Decision Makers at organizations with fewer than 10,000 employees are less apt to fully understand these actors' motives compared to larger organizations with 10,000 or more employees.

Figure 2.4
GREATEST THREAT TO ORGANIZATION

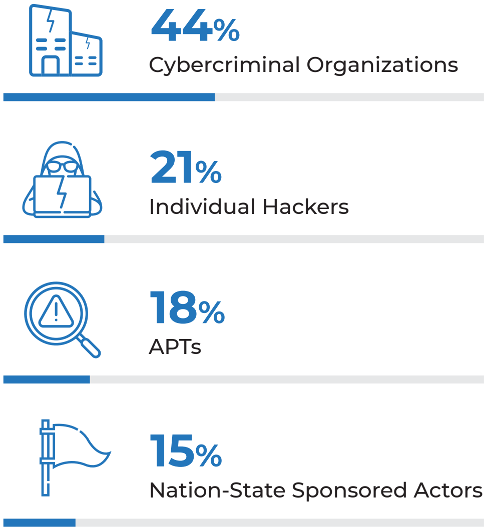
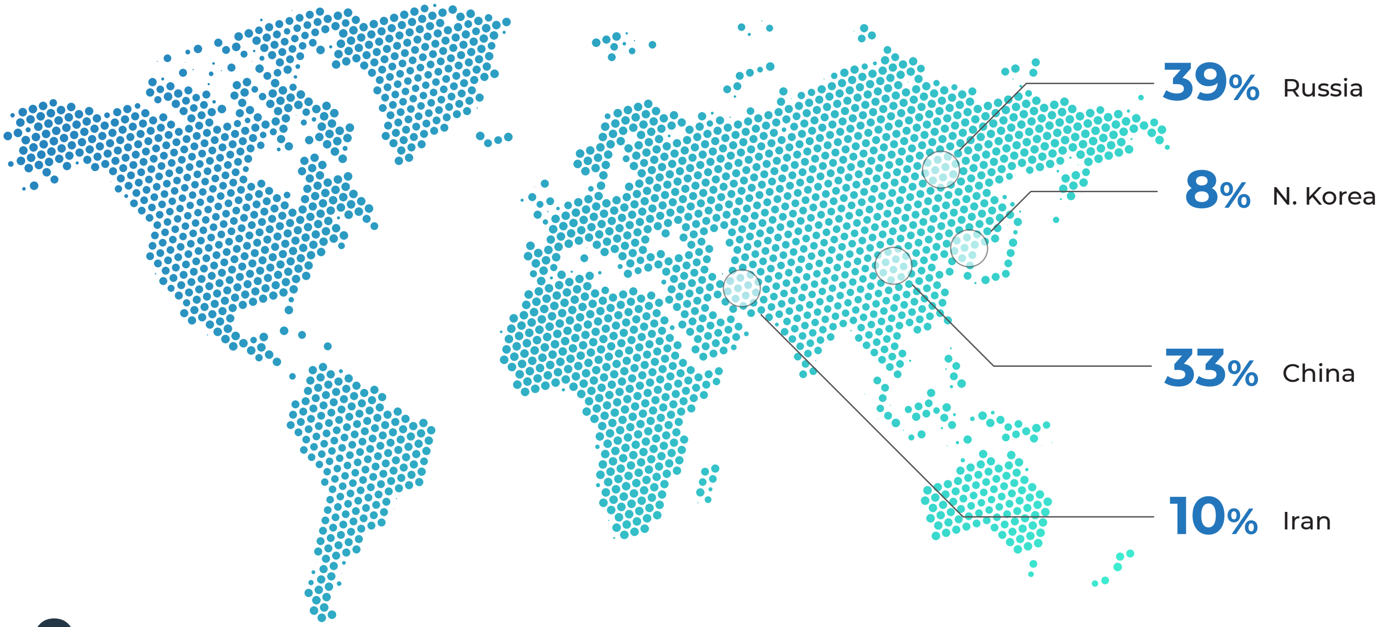


Figure 2.5
COUNTRY WHICH POSES GREATEST CYBERSECURITY THREAT



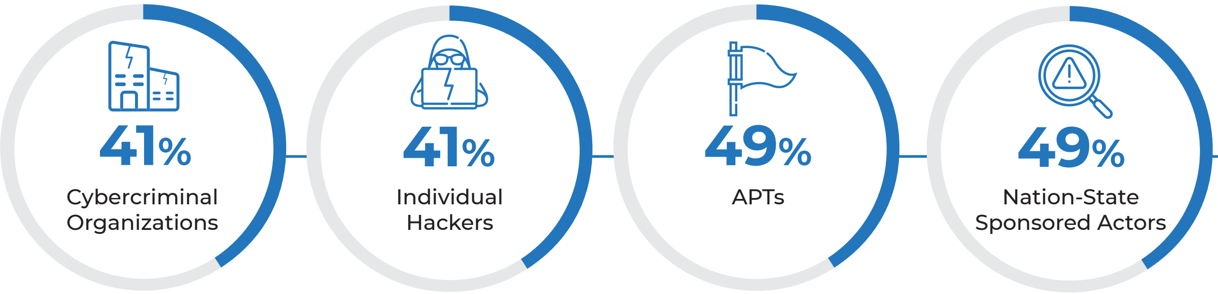
Finding 9

Nearly Half of Enterprise Security Decision Makers Admit They Don’t Understand Adversaries’ Motives Very Well

The persistent noise from threat actors of lower to mid-level sophistication can make indicators of compromise (IOCs) seem like a drop in the ocean. While all this is occurring, more sophisticated groups can hide in the noise while creating custom tools and malware, or abusing legitimate software, to conduct targeted attacks. Therefore, it is crucial to understand threat actors’ motives to know how they work and which may target your organization.

Figure 2.6

PERCENTAGE OF SECURITY DECISION MAKERS WHO DO NOT UNDERSTAND VERY WELL ADVERSARIES' MOTIVES, TACTICS, TECHNIQUES, & PROCEDURES



Those at financial and professional services firms are the most likely to believe they understand cybercriminals’ motivations very well (64% and 65%, respectively), while those at healthcare organizations are the least likely to have this understanding (45%).

THREAT ACTORS: GETTING MORE PRECISE

Anomali Threat Research developed this dashboard to show how to manage threat intelligence to cast a wide initial net and summarize data. With this level of precision, it is easier to understand threat actors’ motives and objectives. In this case, we applied the dashboard to **Mummy Spider**, a cybercriminal group linked to the development of the malware commonly known as Emotet or Geodo.

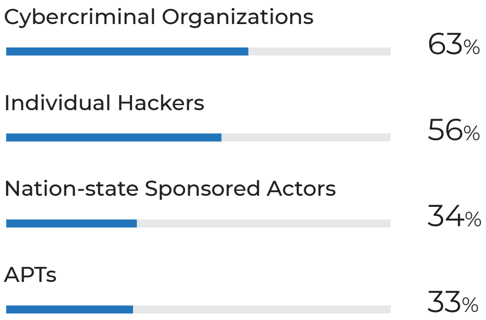
Finding 10

Nearly 9 in 10 (87%) Organizations Have Been Victim to Some Type of Cyberattack in the Past Three Years

Among this group, more than half were hit by cybercriminal organizations and individual hackers. A third were targets of nation-state backed actors and attacks from advanced persistent threats (APTs).

Figure 2.7

SUCCESSFULLY LAUNCHED CYBERATTACK AGAINST ORGANIZATION



Finding 11

Around Half of All Organizations (52%) Have Been Hit by Ransomware Attacks in the Past Three Years

Roughly 40 percent of those struck paid a ransom (39%), with one in five (19%) companies spending $500,000 or more. Despite being one of the most pervasive and well-known threats, ransomware continues to wreak havoc among all organizations. To protect against it, organizations need to know where their vulnerabilities are, properly segment networks, restrict and monitor user permissions, keep backups, and gain the ability to detect and respond to ransomware before it enters networks.

39%

Paid ransom for ransomware attack in the last 3 years

Figure 2.8

AMOUNT PAID IN RANSOM (US CURRENCY EQUIVALENT)

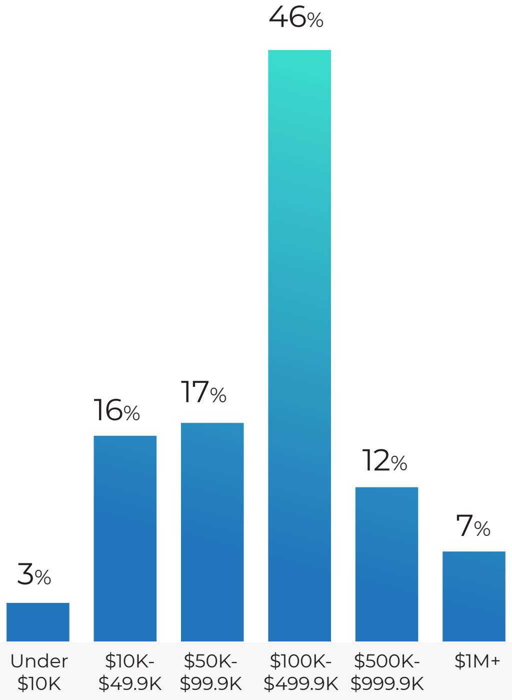
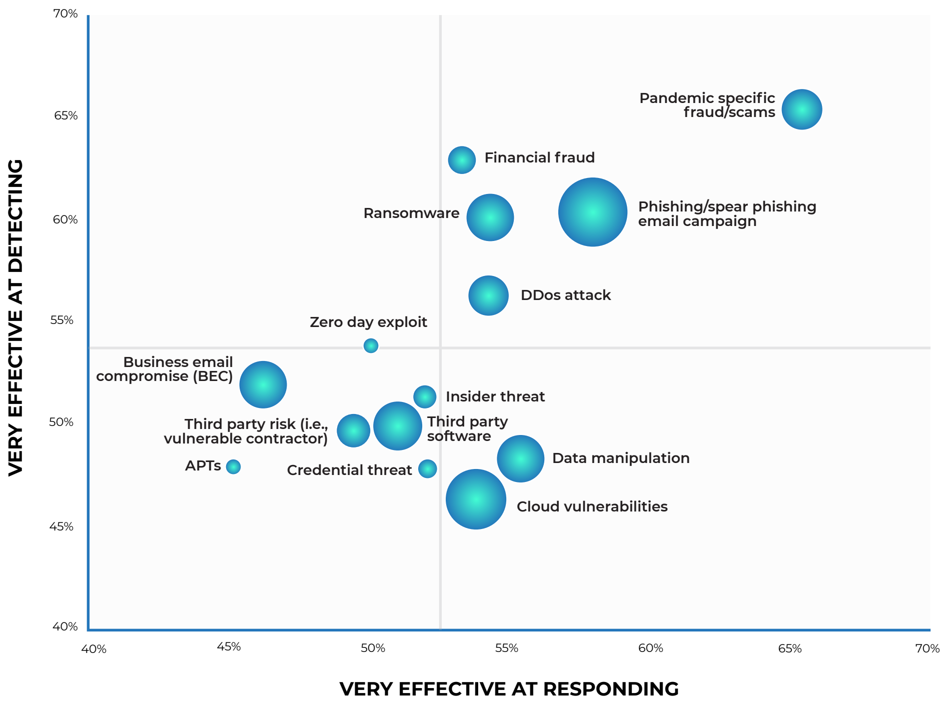


Figure 2.9
POTENTIAL VULNERABILITY AREAS



NOTE: Size of bubble represent frequency of threat occurring in the last 3 years

When the pandemic began, Anomali threat intel analysts detected **6,200 Indicators of Compromise (IOCs) and at least 15 distinct campaigns**. These were associated with 11 threat actors or groups distributing 39 different malware families using 80 various MITRE ATT&CK techniques. Anomali assessed early on that the threat presented by COVID-19-related phishing campaigns against public and private enterprises would continue to rise, with Findings 6 and 7 showing that such attacks are intensifying.

Seventeen percent of organizations have experienced an APT attack in the past three years, and roughly the same proportion (18%) view APTs as the greatest threat to their organization's cybersecurity. Enterprise Security Decision Makers feel they are less equipped to deal with these threats than other types of cyberattacks, with comparatively few saying their organizations are very effective at detecting (45%) and responding (48%) to APTs.

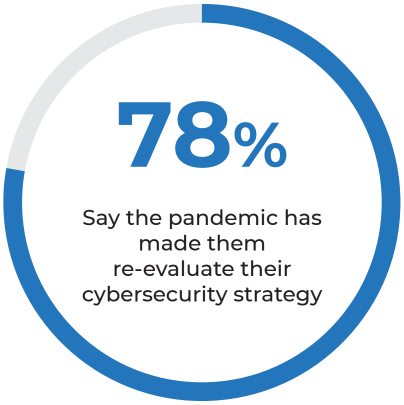
Finding 12

The Pandemic has Forced Organizations to Re-evaluate Cybersecurity Strategies

More than 3 in 4 (78%) Enterprise Security Decision Makers say the pandemic has driven them to re-think their cybersecurity strategies. In our view, this is happening for several reasons. Digital transformation projects, growing remote workforces, and corresponding cloud infrastructure expansion have increased the attack surface faster than it was growing before the pandemic. These factors have forced organizations to increase visibility over their systems, which helps explain planned investments and existing usage in things like XDR, MITRE ATT&CK, and Threat Intelligence (Finding 13). In addition, COVID-19 has given threat actors a recognizable theme to run phishing campaigns and other malicious activities, as the pandemic has proven to be a good weapon for instilling confusion, fear, curiosity, and other emotions that lure people into clicking on malicious links. With new COVID variants always appearing, organizations must increase their ability to adapt, especially when it comes to common attacks like phishing email campaigns.

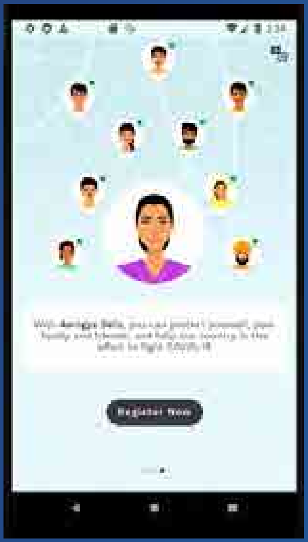
Figure 3.1

PANDEMIC IMPACT ON CYBERSECURITY STRATEGY

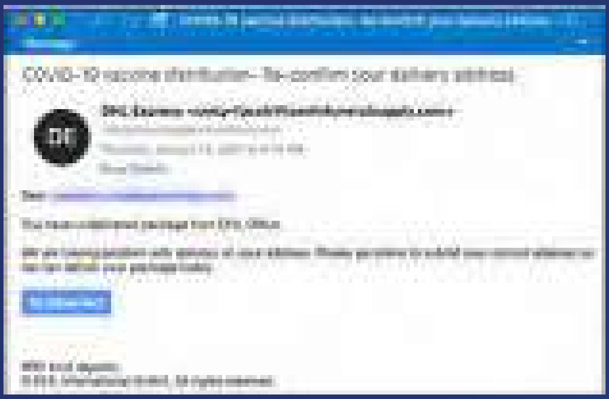


GLOBAL PANDEMIC GIVES ATTACKERS AN EDGE

Since the beginning of COVID-19, Anomali Threat Research has observed and detected many malicious campaigns leveraging the global pandemic as a lure. The image on the right shows an example of a fake COVID-19 mobile device application circulated in the wild as early as June 2020. To help the security community and consumers remain protected against these kinds of fraudulent attempts to spread malware, Anomali threat intel analysts published a detailed blog on the topic: *Anomali Threat Research Identifies Fake COVID-19 Contact Tracing Apps Used to Download Malware that Monitors Devices, Steals Personal Data*



With Aarogya Setu, you can protect yourself, your family and friends, and help our country in the effort to fight COVID-19



COVID-19 vaccine distribution– Re-confirm your delivery address

[illegible]

In addition to fake COVID-19 contact tracing apps, Anomali threat intel analysts have also detected email phishing campaigns leveraging the pandemic theme. The email on the left was detected in Feb. 2021.

Credit: Threat Actors Capitalize on COVID-19 Vaccine News to Run Campaigns, AWS Abused to Host Malicious PDFs, via Anomali Threat Research

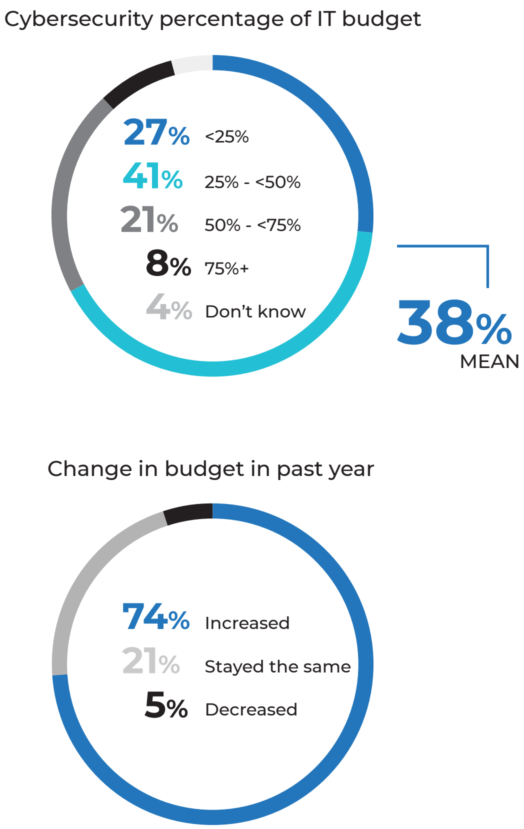
Finding 13

The Financial Impact of Cyberthreats Can be Measured Both in Terms of Rising Cybersecurity Budgets and Direct Losses from Cyber Incidents and Ransomware Attacks

Organizations must maintain a robust defensive posture to protect against a wide array of cyberthreats ranging from phishing email campaigns, cloud vulnerabilities, ransomware, and APTs. Companies are now devoting nearly 40 percent of their IT budgets to cybersecurity (38%), and three out of four (74%) Enterprise Security Decision Makers say that budgets have increased over the past year.

Yet despite this level of spending, direct losses from cyber incidents continue to mount. In 2019, only about a third of businesses globally (36%) reported losses of $100,000 or more (US Currency Equivalent). In 2020 that level rose to almost half (47%). Reported losses of $500,000 or more and $1 million or more doubled over this same one-year period (Losses of $500,000 or more: 15% in 2019 vs. 28% in 2020; Losses of $1 million or more: 5% in 2019 vs. 11% in 2020). 2021 figures were not available at the time the survey was conducted.

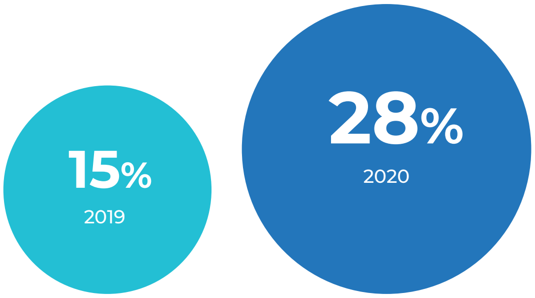
Figure 3.2
CYBERSECURITY BUDGET



Cybersecurity percentage of IT budget

Change in budget in past year

Figure 3.3
ORGANIZATIONS LOSSES OVER $500K DUE TO CYBERATTACKS (US CURRENCY EQUIVALENT)



Ransomware attacks have also become quite costly. Among the roughly two in five (39%) organizations hit by a ransomware attack and chose to pay a ransom, nearly two-thirds (65%) paid out $100,000 or more in US equivalent dollars.

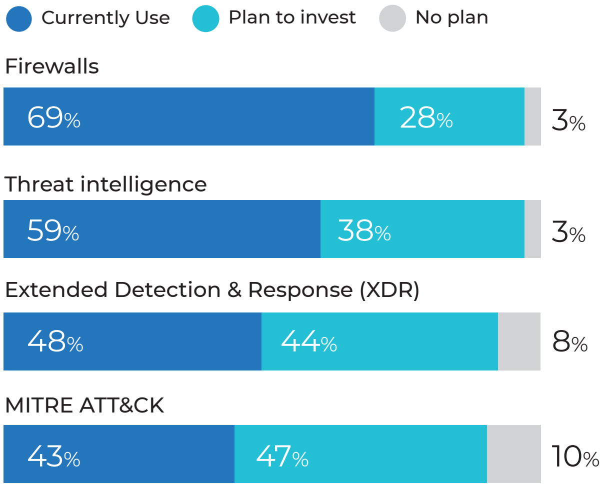
Finding 14

Organizations Continue Using Legacy Technology but are Leaning into New Innovations

Seven out of 10 (69%) organizations still use firewalls to detect threats in the network. However, 59 percent are using Threat Intelligence (38% plan to invest), 48 percent are using XDR (44% plan to invest), and 43 percent are using the MITRE ATT&CK Framework (47% plan to invest). We believe this shift into using and investing in new tools is based on recognizing that while legacy solutions will continue to play a role in defensive strategies, they can no longer be relied upon solely to detect and respond to evolving threats.

Figure 4.1

CURRENT INNOVATIONS USED



Finding 15

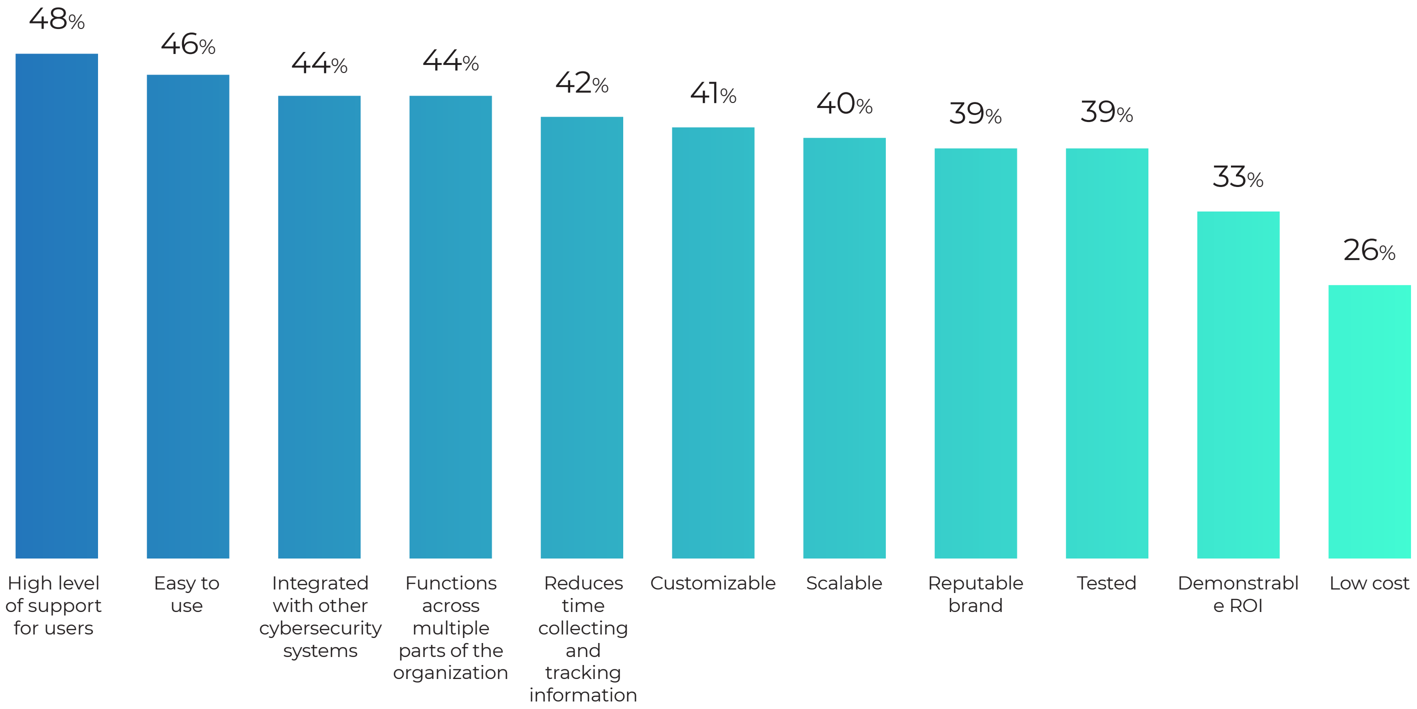
New Cybersecurity Solutions Need to be Integrated into Existing Frameworks and Architectures

To deal with the cyberthreats they face every day, Enterprise Security Decision Makers seek new solutions that are well-supported, easy to use, and integrated with other cybersecurity systems and different parts of their organizations.

Customization and scalability are also considered essential attributes when evaluating new cybersecurity tools by at least four in 10 (41%) decision makers. Nearly as many (39%) want solutions from reputable brands that have been well tested.

Interestingly, only one-third of organizations feel it is essential for a new cybersecurity solution to prove ROI (33%). Low cost is the least of their concerns, with only a quarter of decision makers (26%) citing this as an essential requirement.

Figure 4.2
ESSENTIAL ATTRIBUTES OF EVALUATING CYBERSECURITY SOLUTIONS



Despite findings that show continued over-dependence on legacy technologies, it was encouraging to discover that organizations are either currently using or plan to invest in innovations that can address this problem, such as the MITRE ATT&CK Framework, XDR, and Threat Intelligence.

Finding 16

To Keep Pace with the Threat Landscape, Most Organizations Use Tools and Technologies Designed to Monitor Global Threats

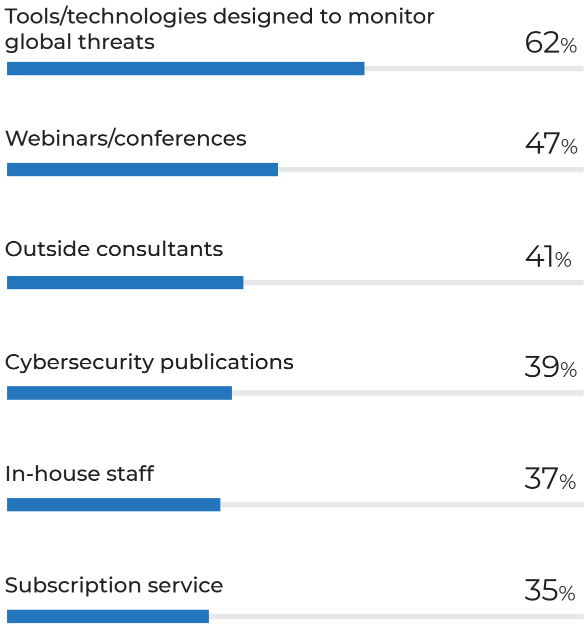
Operationalizing threat intelligence is increasingly critical to an enterprise's ability to manage cyber risk and to build cyber resilience. Security teams can often become overwhelmed by the amount of data they've collected as well as the alerts they receive. With the ability to respond to threats relevant to their specific digital footprint, they become more effective and efficient.

According to the research, 62% of organizations are using tools and technologies to keep an eye on global threats and accelerate their threat intelligence performance. This finding aligns with industry metrics showing that demand is rising for Threat Management Platforms that use global intelligence to detect threats, and other technologies that help automate the collection and correlation of data to make it operational for security teams.

These tools also provide processes for intelligence professionals to manage stakeholder requirements, maximize data analysis by understanding adversaries' intent and objectives, and forecast and improve decision making.

Cybersecurity is now an essential business strategy. Understanding cybersecurity threats and mitigating them requires the right tools, knowledge, and expertise. An effective threat intelligence program helps organizations detect threats early and enables them to act against them quickly.

Figure 4.3
WAYS ORGANIZATIONS KEEP UP WITH THE RAPIDLY CHANGING THREAT LANDSCAPE



CONCLUSION

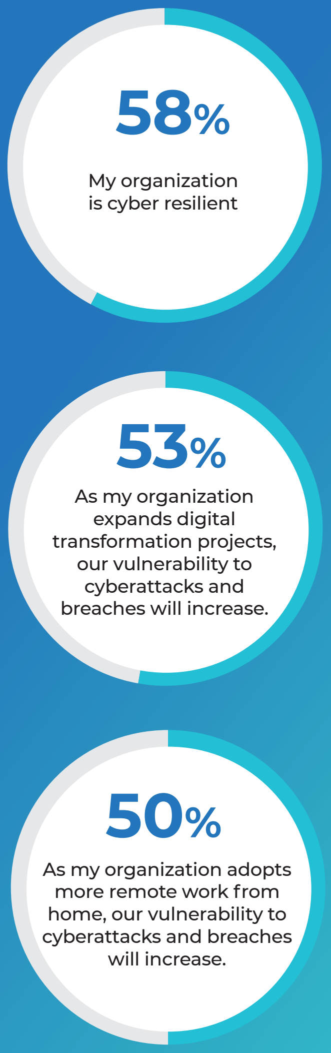
The Level of Cyber Resilience Organizations Have Achieved

For this survey, we defined Cyber Resilience as the ability to proactively and reactively protect your organization against threats and attackers, adapt to changing circumstances during an attack, and recover after a cyberattack has occurred. We found that although organizations are increasing cybersecurity budgets, adding innovative security layers, and focusing on efficacy over costs, they still have much work to do if they hope to thrive in the future.

After almost two years of unprecedented challenges and disruptions to our work and personal lives, some Enterprise Security Decision Makers believe they are progressing, but we can't conclude this is the case. Although 6 in 10 (58%) decision makers strongly agree their organizations are cyber resilient, 87 percent have been the victim of a successful cyberattack over the past three years that resulted in damage, disruption, or a breach to their business. The 42 percent who feel they haven't achieved a level of resilience needed may be more accurately assessing their security postures. Around half of security decision makers, even those claiming to have attained resilience, expressed that expanding digital transformation projects and ongoing remote work will increase their likelihood of falling victim to an attack.

Figure 5.1

ORGANIZATION'S CYBER RESILIENCY (STRONGLY AGREE)



ABOUT ANOMALI

Anomali is the leader in intelligence-driven extended detection and response (XDR) cybersecurity solutions. Anchored by big data management and refined by artificial intelligence and machine learning, the Anomali platform delivers proprietary capabilities that correlate an extraordinary volume of telemetry from customer-deployed security solutions with the largest repository of global intelligence, empowering security operations teams to detect threats with precision, optimize response, achieve resiliency, and stop attackers and breaches. Our Cloud-first SaaS-based solutions easily integrate into existing security tech stacks and accommodate hybrid deployment. Founded in 2013, Anomali serves public and private sector organizations, ISACs, MSSPs, and Global 1000 customers worldwide in every major industry. Leading venture firms including Google Ventures, General Catalyst, and IVP back Anomali. Learn more at www.anomali.com.

HOW ANOMALI HELPS

Cybercriminals, actors backed by nation states, and hacktivists are working overtime to target organizations for exploitation. Organizations need threat intelligence data and insights to fully understand their vulnerabilities to stay ahead of threats and respond to events quickly.

Anomali's intelligence-driven extended detection and response (XDR) provides security teams with the context needed to prevent and address threats more rapidly and effectively. By automating the process of collecting and analyzing internal and external threat data, information, and intelligence, security teams can quickly understand threats, determine impact, and inform an optimized response.

ANOMALI PRODUCTS

Anomali ThreatStream

Threat Intelligence Management that automates the collection and processing of raw data and transforms it into actionable threat intelligence to speed detection, streamline investigations, and increase analyst productivity.

Anomali Match

Intelligence-driven extended detection and response (XDR) that helps organizations quickly detect and respond to threats in real-time. Match automatically correlates ALL security telemetry against active threat intelligence to deliver over 190 trillion threat events per second to expose known and unknown threats to stop breaches and attackers.

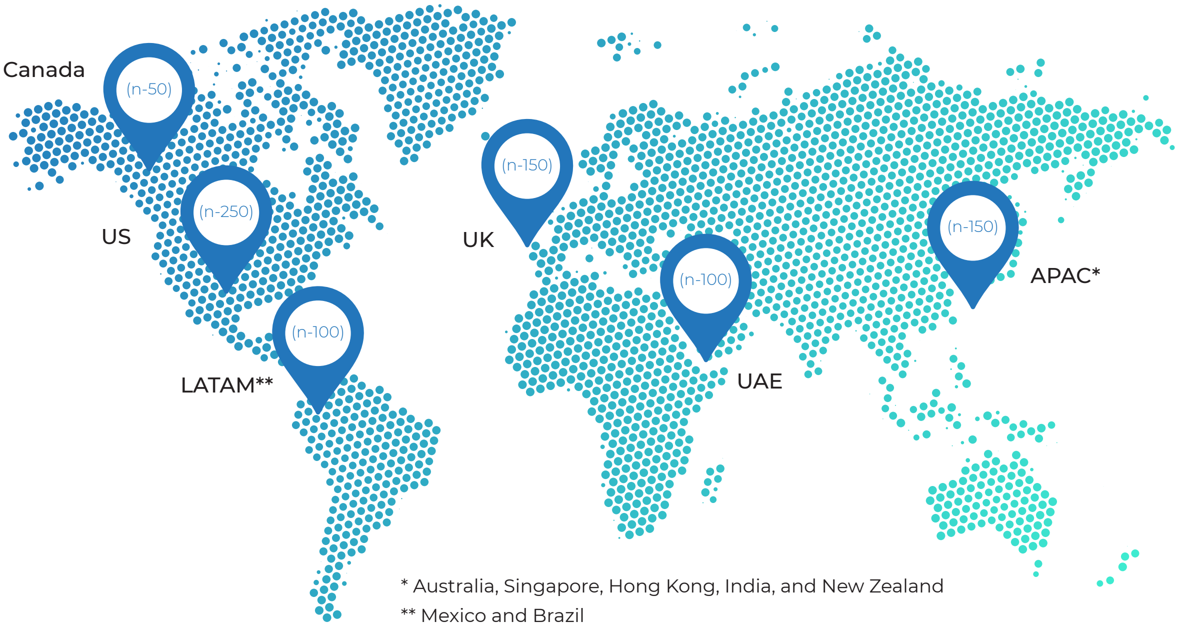
Anomali Lens

Natural Language Processing (NLP) extension that helps operationalize threat intelligence by automatically scanning web-based content to identify relevant threats and streamline the lifecycle of researching and reporting on them.

To find out how Anomali can help your organization become cyber resilient, visit us at **anomali.com.**

Methodology

Anomali commissioned The Harris Poll to conduct online surveys among Enterprise Security Decision Makers in organizations with 5,000+ employees. The survey was fielded between September 9 – October 13, 2021, in the following countries:



* Australia, Singapore, Hong Kong, India, and New Zealand

** Mexico and Brazil

QUALIFICATION CRITERIA

- Age **18+**
- **Employed full-time**
- In **financial services, pharma, healthcare, telecom, manufacturing, professional service**
- In an **IT role**
- **Technology perspective:** Manager level+ and have influence on data security solutions
- **Business perspective:** Director level+ and have influence over data security strategy

Raw data were weighted where necessary by the number of businesses within employee size class to bring them in line with their actual proportions in the population of businesses with 5000+ employees in the select industries of Manufacturing, Telecommunications, Financial Services, Healthcare, Pharmaceuticals, and Professional, Scientific & Technical Services, for each country separately. The countries were then combined using a post weight to proportion them equally in the Total.