2020

CYBERSECURITY REPORT CARD

Organizations Rate Their Security Posture and Put Assumptions to the Test

2020 has been a year filled with uncertainty. Many industries were either unprepared or not designed to move to a fully remote work environment with haste. Those on the cyber defense frontlines were faced with new challenges in multiple areas as an increase in cyber attacks coincided with the sudden shift to remote work.

The progress made over the previous years towards a more mature security posture equipped many organizations with the skills and tools to meet these challenges head on. As a result, the number of reported breaches this year did not increase, despite the pandemic.

This paper outlines the results of the DomainTools' fourth annual Cybersecurity Report Card Survey. More than 520 security professionals from companies ranging in size, industry, and geography were surveyed about their security posture and asked to grade the overall health of their programs. Almost 60 percent of respondents are on the cyber frontlines as security researchers, analysts or threat hunters. The responses built on the results of the previous **2017**, **2018**, and **2019** Report Cards. The environment that this year's survey was conducted in differs markedly from previous years due to the upheaval that arose from the global pandemic.

Summary Highlights

The report finds that confidence in cybersecurity programs continues to remain steadfast despite the challenges brought on by COVID-19. Twenty-four percent of respondents gave their program an “A” rating, a decrease from 30 percent in 2019. However, this was offset by increases to both grade “B” and “C” categories.

The percentage of organizations that have been breached in the past 12 months remained essentially unchanged at 16 percent. While this marks the first time that the incidences of reported breaches have not declined, this finding can be seen as a success given that security teams detected a significant increase in the number of attacks related to the pandemic. Automation played a key role in securing organizations during the year as 75 percent reported that automation has improved their ability to transition to a secure remote workforce during the pandemic.

Key Findings

An Inflection Point Year

Cybersecurity report card grades showed a slight decrease in improvement in 2020, with 24 percent giving their programs an “A,” down nearly 6 percent from 2019. Half of all respondents now stand solidly as a “B,” and a quarter as a “C.” The “D” grades remained unchanged and grade “F” was reduced to zero. Though the grades were slightly restructured from the previous year, this does not mean cybersecurity programs have weakened. The number of reported breaches still remains 10 percent lower than the 26 percent recorded in 2017.

The COVID-19 Crises

COVID-19 set the stage for an unprecedented rise in global cyber attacks as cybercriminals sought to capitalize on the state of uncertainty across the world. Nearly 60 percent of organizations detected a moderate to a dramatic increase in cyber attacks during and following the pandemic and three-fourths of respondents detected COVID-19 specific threats at least several times per month.

The Remote Work Challenge

The majority of security teams report being well prepared to handle increased cyber attacks amid new vulnerabilities from remote work due to COVID-19. Continued adoption of automation was key to this transition as over three-fourths of respondents stated that automation has improved their ability to transition to a secure remote workforce during the pandemic.

The Groundwork for Success: Leadership and Training

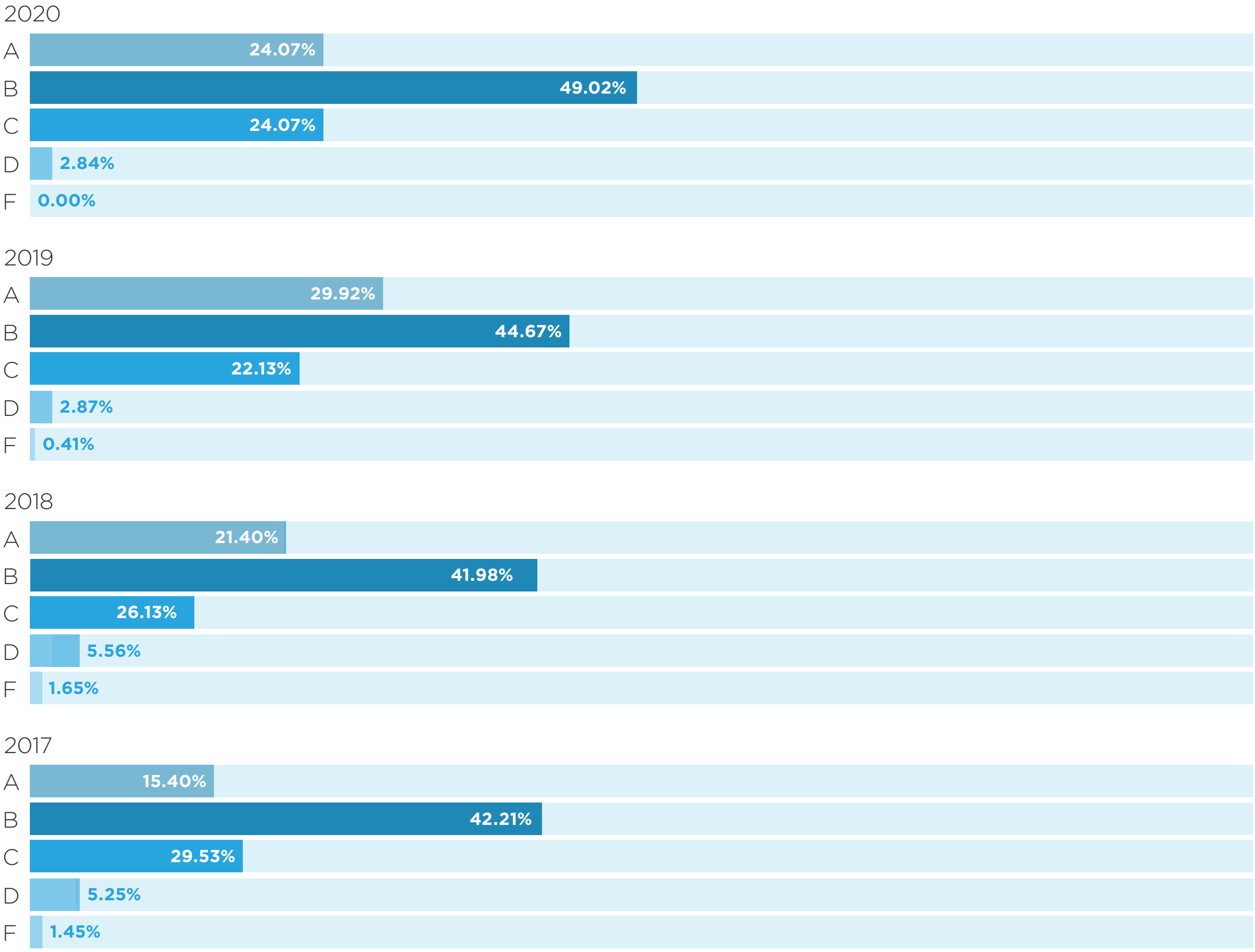
Security teams were able to successfully navigate the pandemic by being properly prepared beforehand and having executive support during the crises. Over 80% of organizations said their training programs properly prepared them to handle the COVID-19 pandemic and nearly half of all respondents gave their CISOs and CEOs an “A” grade for their executive performance in keeping the organization secure.

An Inflection Point Year

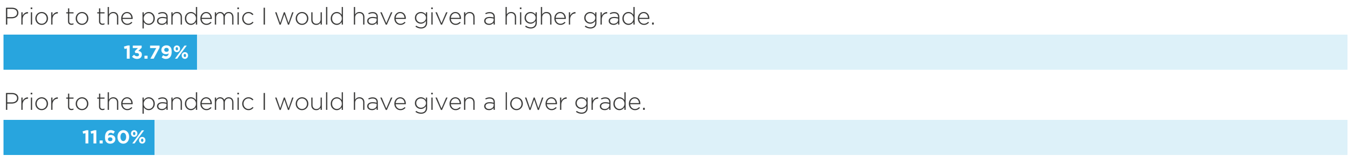
Beginning in 2017, only 15 percent of respondents gave their organization an "A" rating. Last year that number had doubled to 30 percent. For the first time, respondents lowered their grade "A" ratings to 24 percent. However, this was offset by an increase in "B" grades to 49 percent over last year's 45 percent, and a two percent increase in "C" grades over last year to 24 percent. For the first time in the report's four year history, not a single respondent gave their organization an "F" rating.

COVID-19 served as an inflection point for over a quarter of security teams to reassess their perceived cybersecurity posture. Twelve percent of respondents would have given their organization a lower grade prior to the pandemic, showing surprise in how well they were able to cope. The number of reported breaches remained essentially unchanged from 2019 at 16 percent showing that the slight shifting of grades did not detract from cybersecurity resilience.

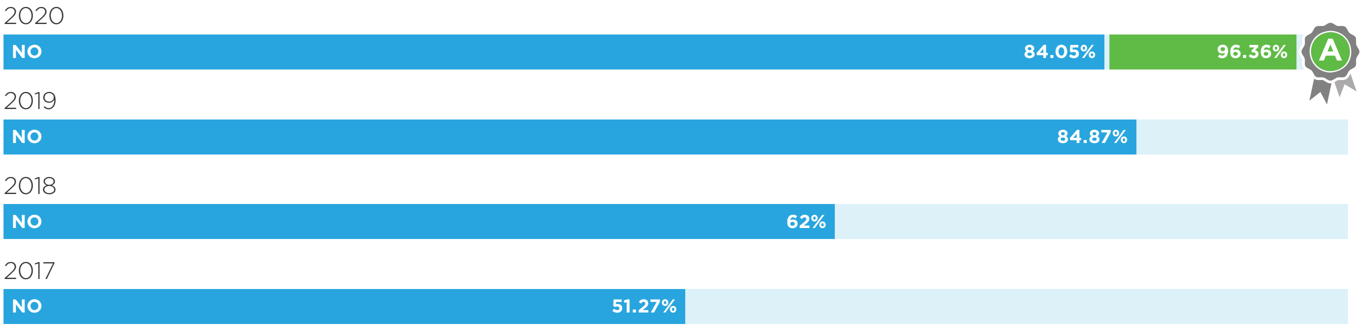
How would you grade your cybersecurity system?



Would your grade have been different prior to the pandemic?



Has your organization been breached in the last 12 months?

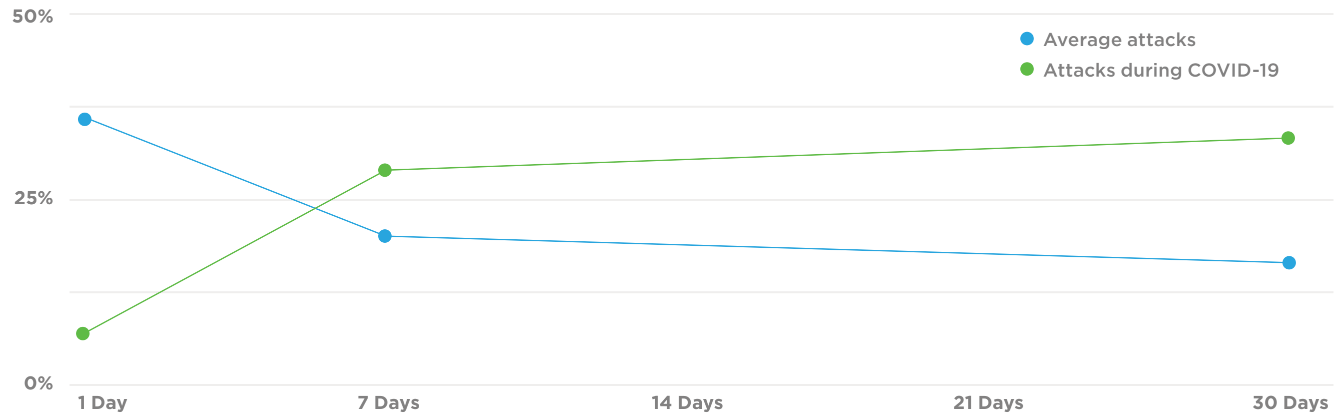


The COVID-19 Crises

Organizations experienced a remarkable increase in the number of cyber attacks during and following the pandemic. On average, 36 percent of organizations detect cyber attacks several times per day. During COVID-19, fourteen percent of survey respondents reported also detecting COVID-specific attacks several times per day. As time went on, the number of COVID-specific threats detected per week (28 percent) and per month (32 percent) increased over the number of general attacks detected per week (22 percent) and per month (20 percent).

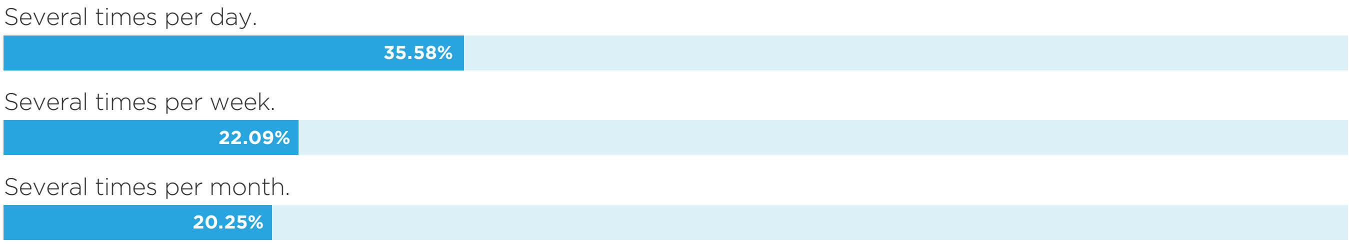
Over half (57 percent) of organizations state they can detect an attack in less than a day, a slight decrease from 60 percent in 2019. However, 35 percent of survey respondents said that the shift to remote working has increased their detection and response time, which correlates with the delay. For the first time, the report measured the average response time post-detection of a security event, with over half (52 percent) of respondents having the ability to respond in less than a day.

Average percentage of cyber attack detections during and following the pandemic.

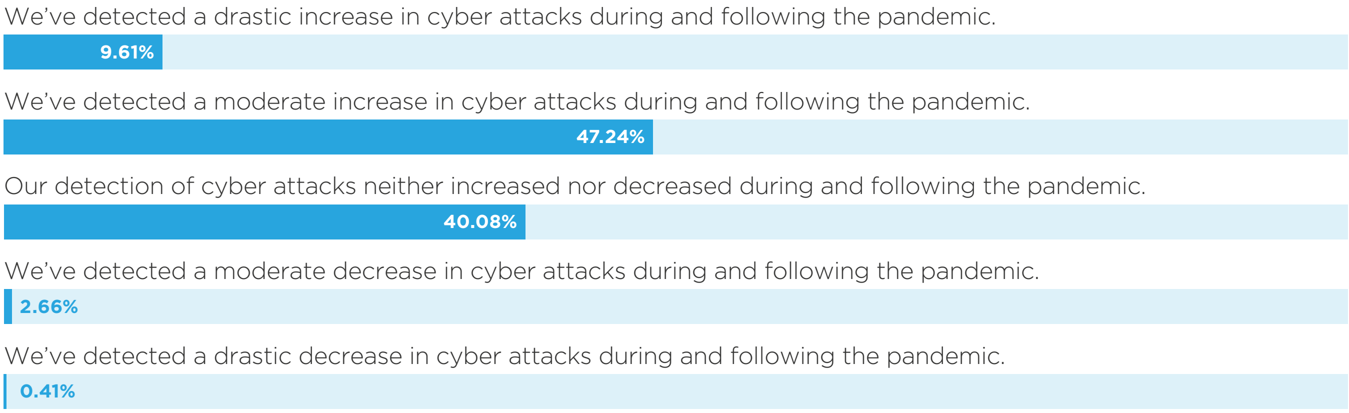


— The COVID-19 Crisis (cont)

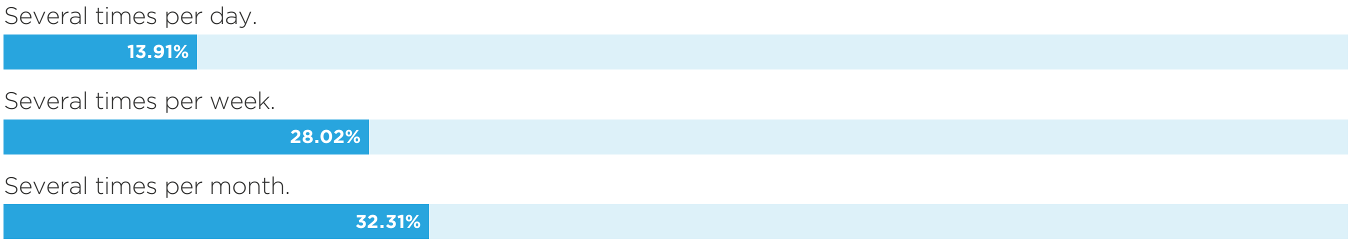
How often does your organization detect active or suspected cyber attacks?



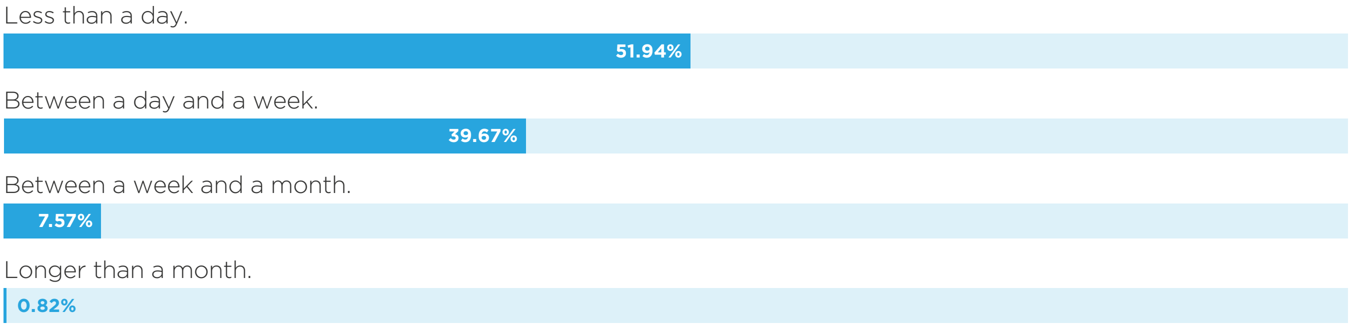
Has COVID-19 affected the number of active or suspected cyber attacks you detect?

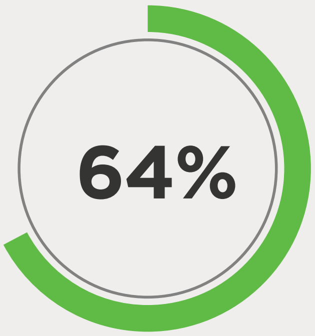


How often do you detect COVID-19 specific threats (i.e. phishing attacks, COVID-specific malware)?

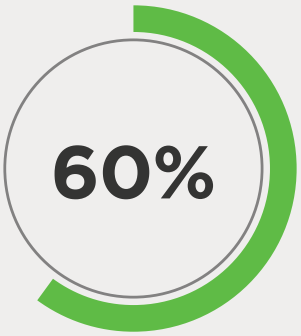


What is your average response time post-detection of a security event?

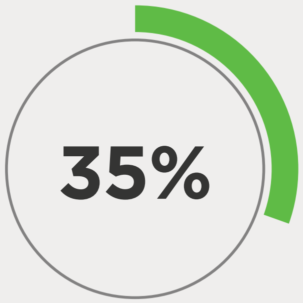




Percentage of organizations that had to set up the infrastructure required to enable a high volume of remote workers.



Percentage of respondents who state that working from home has made their organization more vulnerable to cyber threats.



Percentage of respondents who said their organizations tightened their security policies and settings now that most people are presumably working from home.

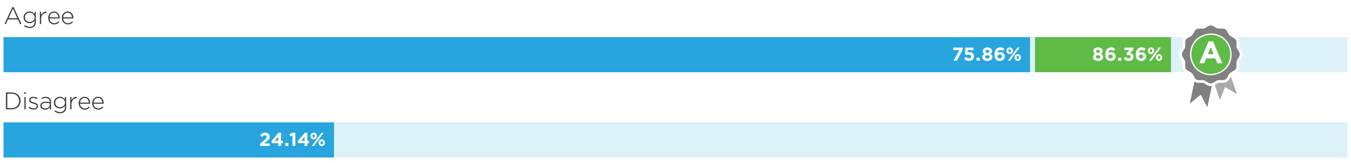
The Remote Work Challenge

COVID-19 forced the adoption of remote work to become the new reality for organizations overnight. While over half (56 percent) of organizations were prepared to enable a fully remote workforce before COVID-19, that still means a sizable amount (44 percent) of organizations were either not prepared or unsure if they were prepared. To meet the needs of remote work, 64 percent of organizations had to set up the infrastructure required to enable a high volume of remote workers.

The increase in cyber attacks along with the sudden shift to remote working had over half (60 percent) of respondents state that working from home has made their organization more vulnerable to cyber threats. Because of this, 35 percent of respondents said their organizations tightened their security policies and settings now that most people are presumably working from home. 11 percent responded that they had loosened their security policies and settings—likely the organizations that were least prepared and had to sacrifice security to enable remote working.

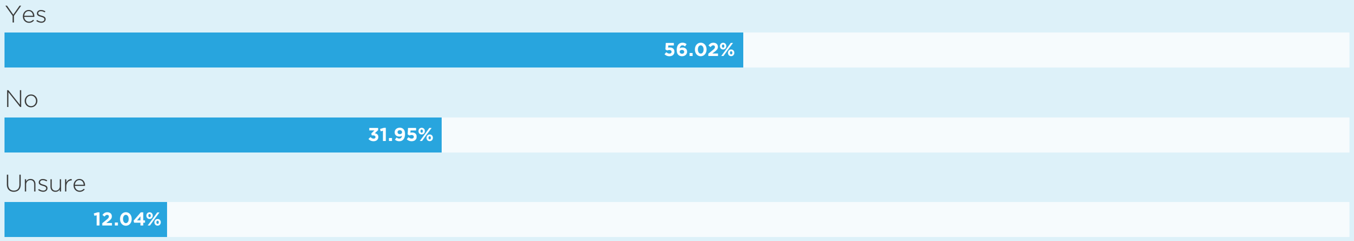
Automation played a key role during this period as 76 percent of respondents agreed that automation improved their ability to transition to a secure remote workforce during the pandemic.

Automation has improved our ability to transition to a secure remote workforce during the pandemic.

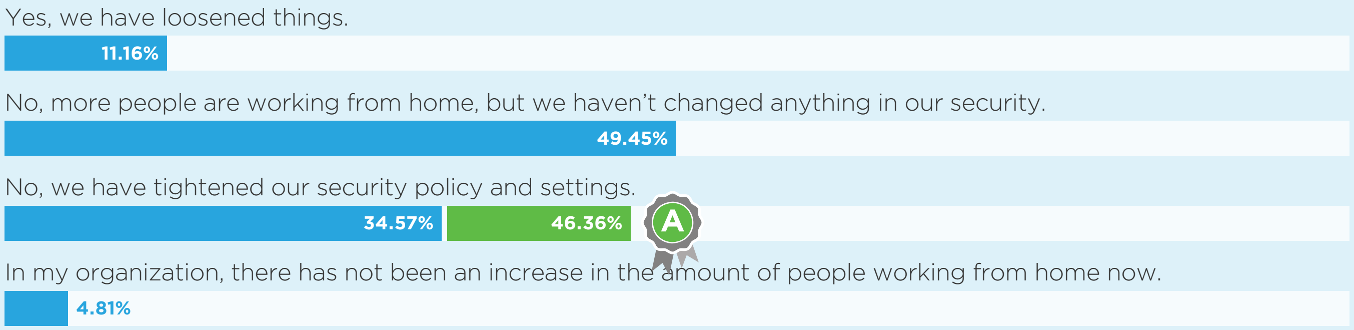


— The Remote Work Challenge (cont)

Was your organization prepared to enable a fully remote workforce before the pandemic?



Has your organization loosened its security policies and settings now that most people are presumably working from home?

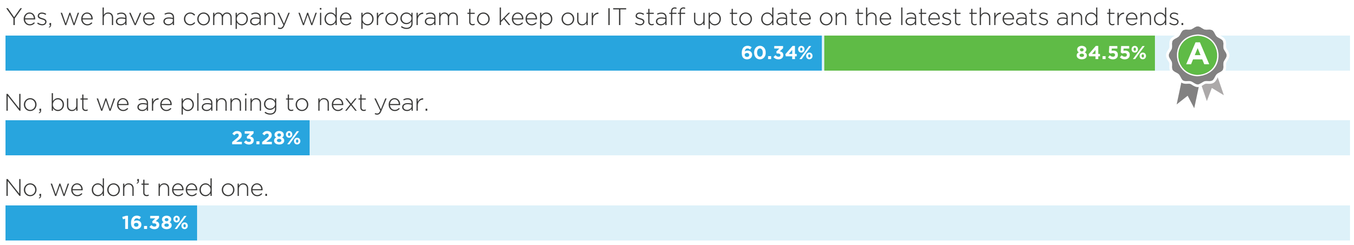


The Groundwork for Success: Leadership and Training

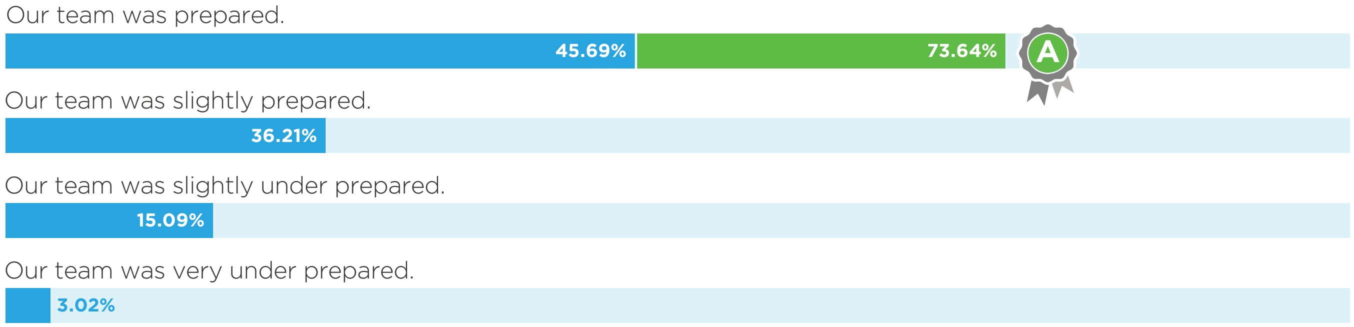
Company wide programs to keep security staff up to date on the latest threats and trends are up over 10 percent since 2017 to 60 percent today. Formalized training programs proved their worth during COVID-19. 46 percent of respondents said the training offered by their organization well-prepared them to handle an event like the pandemic, and 36 percent said the training slightly prepared them. Nearly a quarter of respondents said they plan to implement a training program next year.

The majority of respondents cited strong leadership at the executive level as a factor that kept their organization secure during the pandemic. 45 percent of respondents gave their CISO/security manager's ability to maintain the security posture of their organization during the pandemic an "A" while 37 percent gave a "B" grade. The CEO's support of the security team during COVID-19 also received high marks. 48 percent of CEOs received an "A" grade and 32 percent got a "B" rating.

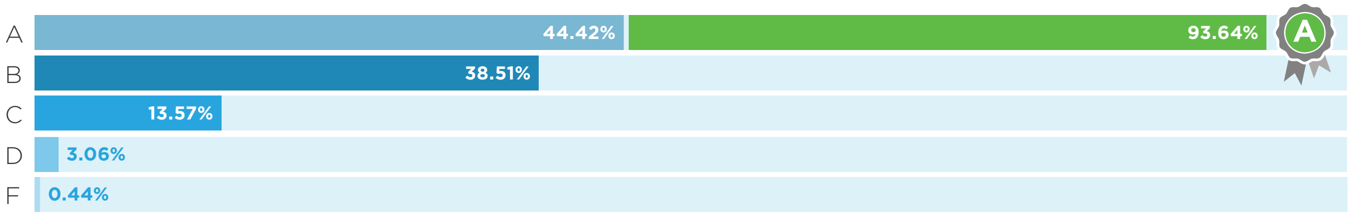
Do you have a formalized training program for your IT staff?



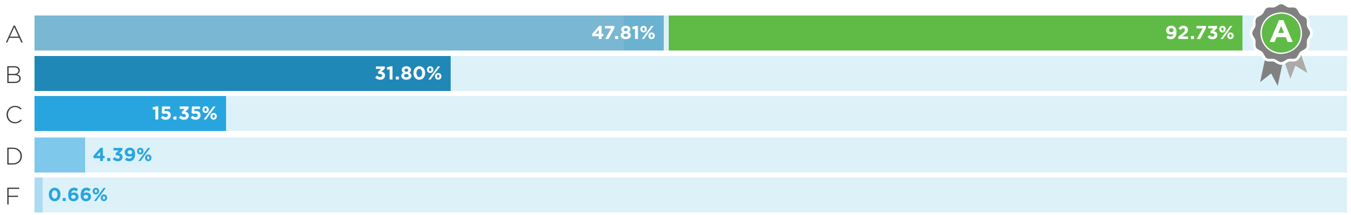
Did the training offered by your organization prepare you to handle an event like the pandemic?



What grade would you give your CISO/security manager's ability to maintain the security posture of your organization during the pandemic?



What grade would you give your CEO's support of the security team during the pandemic?



Common Attacks See Shift in Spearphishing

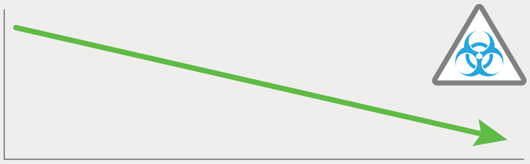
Common threat vectors remain steady year over year, with Business Email Compromise and malware at the top of the list, while spearphishing shifted to the top of the list this year, up 24 percent from last year.

TOP 3 Most Common Attacks Detected

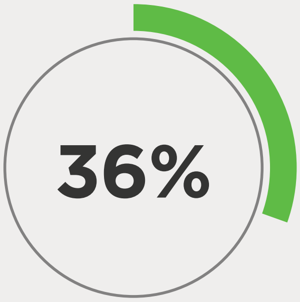
1 **85%** **Spearphishing**

2 **46%** **Malware**

3 **38%** **Business Email Compromise**



On the steady decline: malware fell 28 percent from last year.



Percentage of organizations that detect active or suspected cyber attacks several times a day (vs. week, month or year and a slight decrease of 4 percent over 2019)

Post-COVID in 2021

One of the most important indicators of the future of cybersecurity may be in how COVID-19 has impacted security budgets.

Nearly 40 percent of organizations have changed their security budgets following the pandemic. Almost a quarter of organizations (23 percent) have increased their security budget. This is likely from organizations that plan to take a proactive approach to bolstering their security programs so they are even better prepared for the future.

For organizations that have increased their security budget, they plan to spend the majority of the money on increasing their team's headcount (54 percent), investing in training for team members (48 percent), and adding new threat intelligence sources (36 percent).

Surprisingly, fifteen percent of organizations have decreased their security budget. These are likely the organizations that were already under prepared to handle the pandemic and are forced to make cuts to stay afloat or shift spending from security to supporting remote work. This is unfortunately short-sighted as it will likely further exacerbate the inability to protect their organizations.

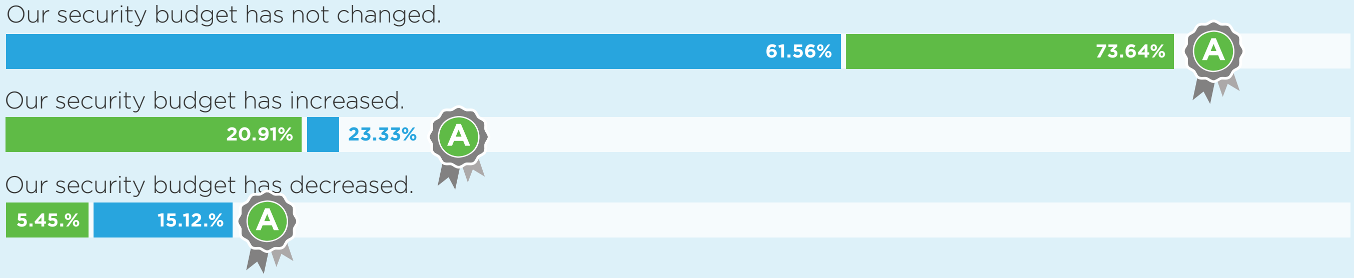
For the organizations that have decreased their security budgets, they plan to cut spending by putting new purchases on hold (59 percent), reducing their team's headcount (21 percent) and consolidating tools and platforms (10 percent).

— Post COVID in 2021 (cont)

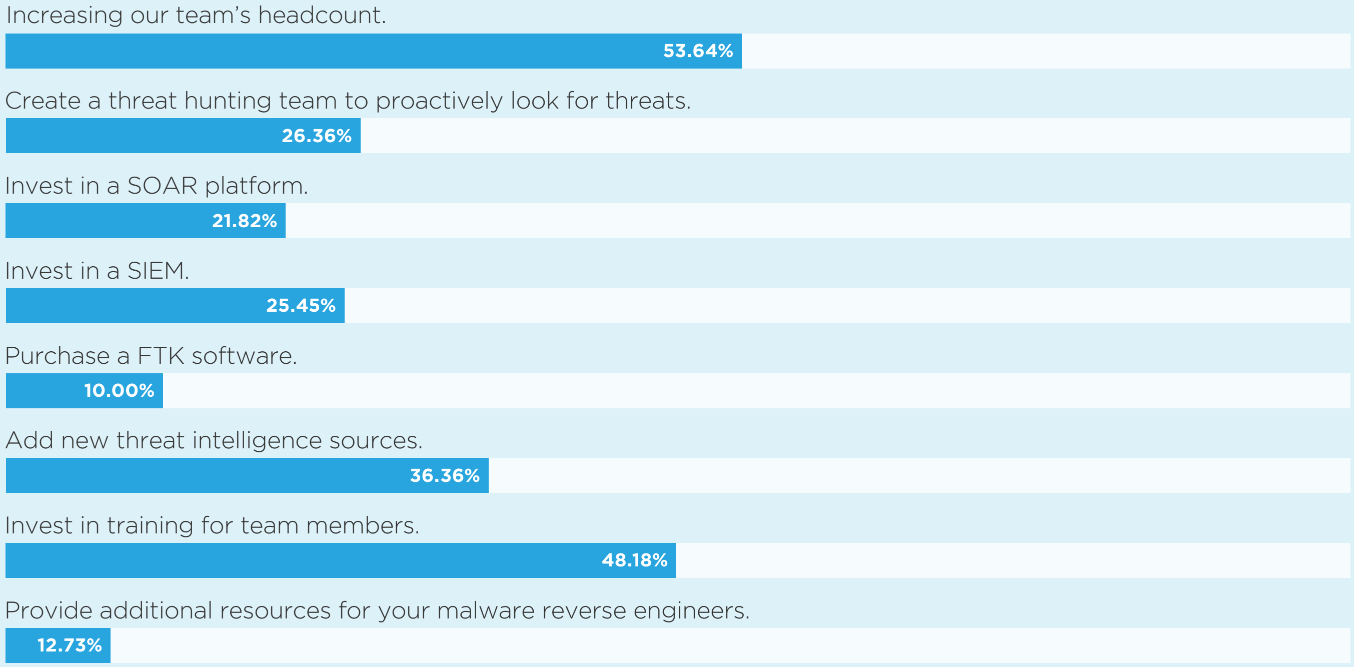
Of those that gave their organizations an "A" grade, nearly 75 percent stated that their security budget has not changed, likely showing that they already had healthy budgets. Those organizations were also 10 percent less likely to see a decrease in their budgets following the pandemic.

Looking ahead into 2021, security teams can learn lessons from the organizations that gave themselves an "A" grade this year: They leveraged automation more than the mean, invested significantly more in formalized training, and graded their executive staff's performance twice as high as other organizations. This led to a greater level of preparedness and a large decrease in the number of reported security breaches.

How has COVID-19 impacted your security budget?

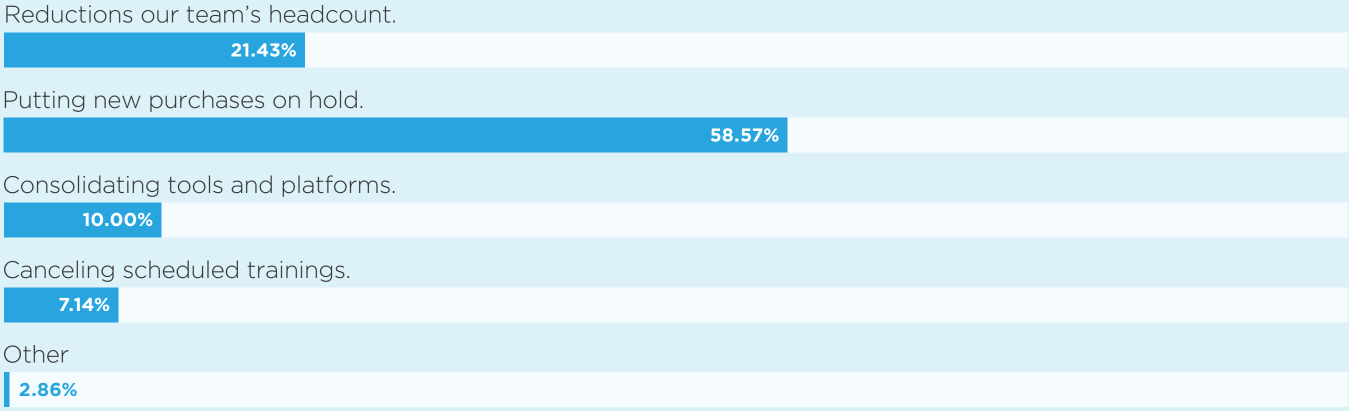


If your security budget has increased, how is your security organization allocating funds?



— Post COVID in 2021 (cont)

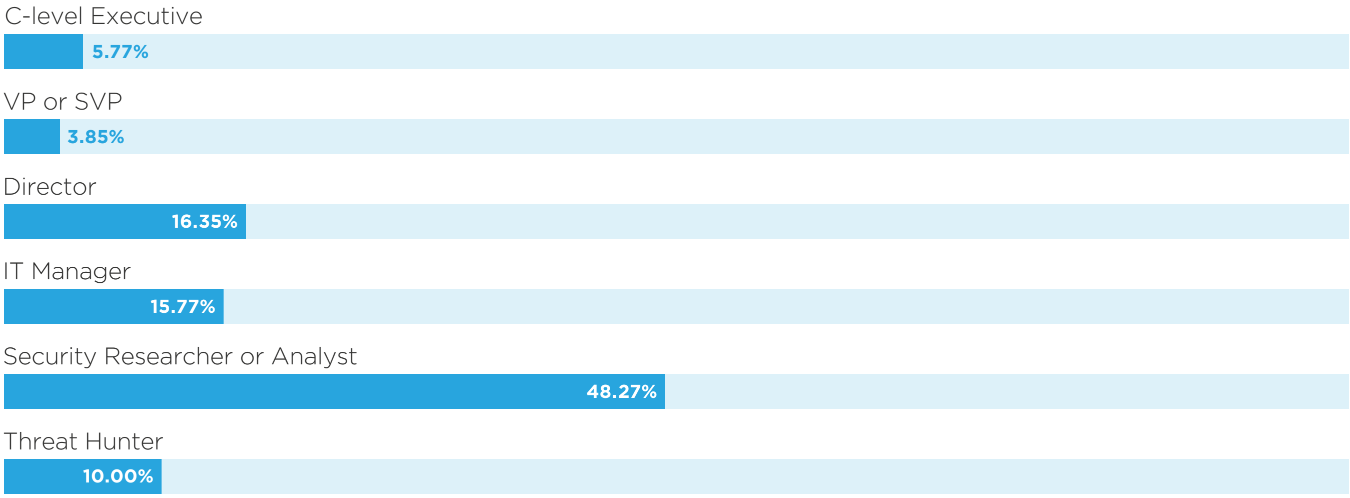
If your security budget has decreased, where are you seeing the most impact?



Methodology

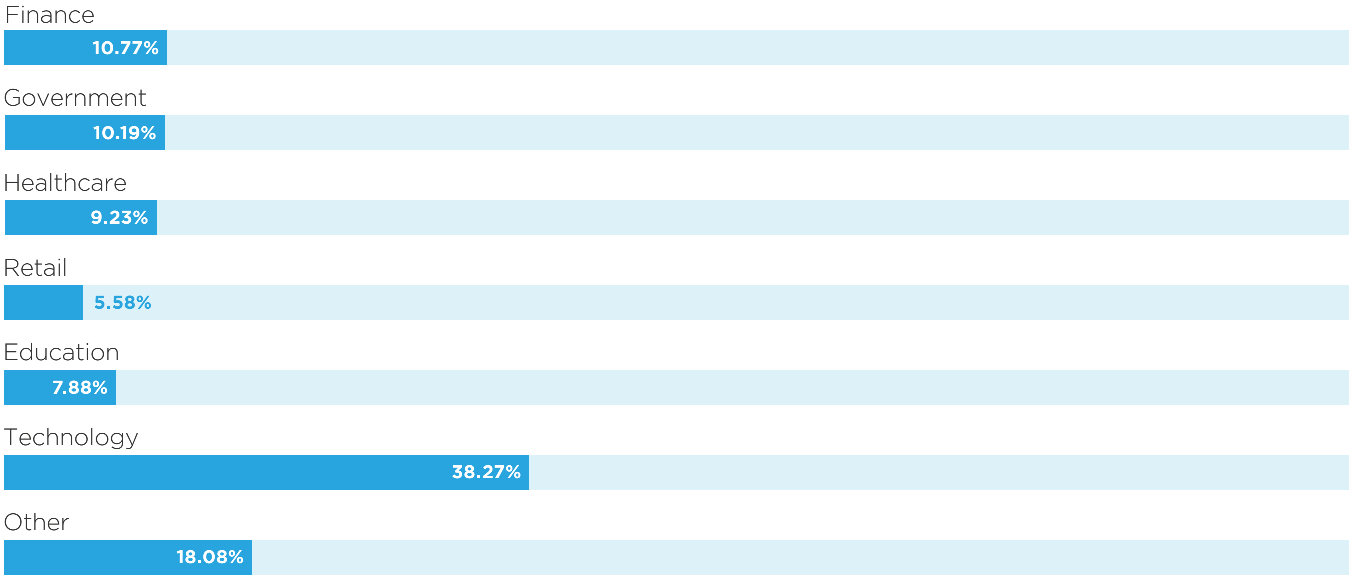
The survey was conducted by DomainTools in September 2020, and polled 520 global security professionals and executives working in finance, government, healthcare, retail, technology and other industries in organizations of up to 10,000+ employees. Regions include North America, EMEA, APAC and LATAM. A breakdown of the respondents' titles, roles and industries are provided below.

What is your title?

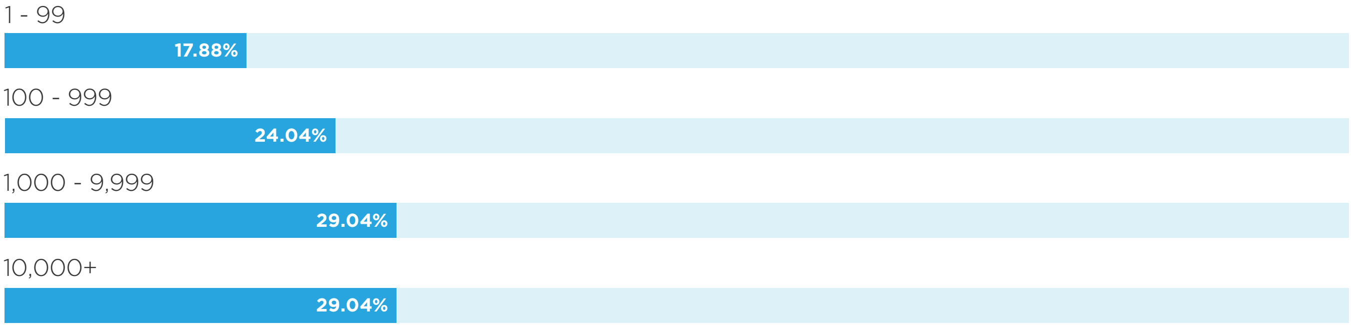


— Methodology (cont)

What is your industry?



How large is your organization?



About DomainTools

DomainTools helps security analysts turn threat data into threat intelligence. We take indicators from your network, including domains and IPs, and connect them with nearly every active domain on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure. Fortune 1000 companies, global government agencies, and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and mitigation work. Learn more about how to connect the dots on malicious activity at **http://www.domaintools.com** or follow us on **Twitter: @domaintools**.