Security Budgets During COVID-19

When lockdown protocols kicked in due to COVID-19's rapid spread all around the world, teams across many industries migrated to a work-from-home normal. However, with remote work comes new security risks—like employees accessing sensitive company assets through personal devices and home wifi.

How have security budgets changed as a result of new and broadening security threats? 200 IT executives share:

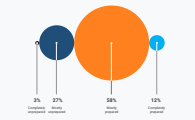
- How security teams transitioned to a remote workforce
- The top security issues they've been facing—and their strategies to tackle them
- How their budgets have been affected, and whether they'll change in 2020

Data collected from June 24 - Aug 31 2020 | Respondents: 200 IT Executives

PREPARATION, PREPARATION... PREPARATION?

When the pandemic hit, 57% of IT execs felt their security team was already prepared to support a remote workforce.

HOW PREPARED WAS YOUR SECURITY TEAM TO SUPPORT A REMOTE WORKFORCE WHEN THE COVID-19 PANDEMIC BEGAN?

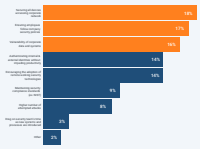


Comparing how different industries responded, 42% of those in the manufacturing industry said their security team wasn't prepared to support a remote workforce when the lockdowns hit. Comparatively, 15% of software execs felt mostly unprepared.

TOP SECURITY HEADACHES ARE ONLY THE NEW-ISH NORMAL

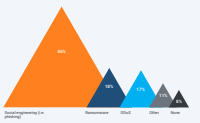
Securing all devices being used to access corporate networks (19%) is the number one security issue teams have faced during COVID-19. Handling employees who don't follow company policy (17%) was a close second.

WHAT ARE THE TOP 3 SECURITY ISSUES YOUR COMPANY HAS FACED DURING THE CRISIS?



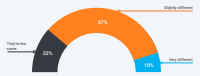
Security leaders are also facing an increasing number of security threats. Phishing, and other social engineering strategies that trick users into providing access to their credentials, accounts for a striking 86% of reported attacks in the past quarter, more than twice as much as ransomware attacks, the next highest at (18%).

WHAT TYPES OF CYBERATTACKS HAVE BEEN LAUNCHED AGAINST YOUR ORGANIZATION IN THE PAST QUARTER?



While these issues have surfaced during the remote working era, the vast majority of execs say these issues are the exact same (33%) or only slightly different (67%) compared to what their security teams were facing in pre-pandemic times.

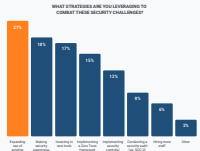
TO WHAT EXTENT ARE THESE ISSUES NEW FOR YOUR ORGANIZATION?



SECURITY STRATEGIES HAVE BEEN VARIED, INVOLVING BOTH NEW TOOLS AND THE TRIED-AND-TRUSTED

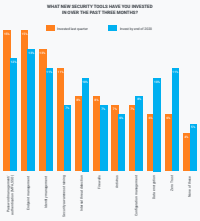
17% of execs are exploring new tools to fight security challenges, but most are expanding their existing toolkit, according to 21% of responses.

WHAT STRATEGIES ARE YOU LEVERAGING TO COMBAT THESE SECURITY CHALLENGES?



The most popular tool categories IT leaders have spent on over the past quarter are password management (13%) and endpoint management (13%). These are also the most popular solutions that will be adopted by the end of the year.

WHAT NEW SECURITY TOOLS HAVE YOU INVESTED IN OVER THE PAST THREE MONTHS?



Zero Trust and data encryption technologies will see the biggest investment spike by the end of the year, increasing in adoption at 9% and 8% respectively.

WHEN IT COMES TO SECURITY, COVID HASN'T IMPACTED BUDGETS, NOR DO EXECS EXPECT IT TO GOING FORWARD

More than two-thirds of IT leaders (69%) say their security budgets either stayed the same or increased last quarter, despite the pandemic. Most leaders don't anticipate these budgets to change for the rest of the year (57%), though 36% are optimistic they'll increase before 2021.

HOW HAS YOUR SECURITY BUDGET CHANGED IN THE PAST QUARTER?

HOW WILL YOUR SECURITY BUDGET CHANGE BY THE END OF 2020?

In addition to growing budgets, most execs (57%) are looking to grow their security team size by the end of the year.

ARE YOU PLANNING TO GROW YOUR SECURITY TEAM IN 2020?

RESPONDENT BREAKDOWN