CYBEREDGE GROUP

THE IMPACT OF COVID-19 ON ENTERPRISE IT SECURITY TEAMS

A Survey of Enterprise IT Security Professionals on the Impact of COVID-19 on IT Security Budgets and Personnel, Challenges of Supporting a Remote Workforce, and New Technology Investments

OCTOBER 2020

A CYBEREDGE RESEARCH STUDY SPONSORED BY:

(ISC)² Gigamon SecurityScorecard thycotic

Introduction **3**
Top Five Insights 3
About This Report 4
Navigating This Report 4
Research Highlights **5**
Section 1: Budgets & Personnel **6**
Impact to 2020 IT Security Operating Budgets 6
Impact to 2021 IT Security Operating Budgets 7
Impact to 2021 IT Security Training & Certification Budgets 8
IT Security Personnel Shortage 9
Workforce Spending Reduction Methods 10
Section 2: Work-from-home Movement **11**
Expanded Remote Workforce 11
Work-from-home Preferences 12
Increased BYOD Policy Adoptions 14
Section 3: IT Security Challenges **15**
Operational Challenges 15
Professional Certification Preparedness 16
Impact to Third-Party Risks 17
Impact to Third-Party Risk Management Programs 18
Third-Party Risk Management Automation 19
Section 4: Technology Investments **20**
Pandemic-fueled Technology Investments 20
Preference for Cloud-based Security Solutions 21
Securing Personally Owned Devices 23
Conclusion **24**
Appendices **26**
Demographics 26
Research Methodology 28
About Our Sponsors 29
About CyberEdge Group 30

Introduction

The Coronavirus disease of 2019 (COVID-19) was first identified in December 2019 in Wuhan, China and has resulted in an ongoing global pandemic. In less than a year, more than 30 million people have been infected and more than 1 million people have died.

Although COVID-19 is often compared with influenza due to its symptom and transmission similarities, it's far more contagious and considerably more deadly. Virtually every country has experienced a lockdown in some form, with federal, state, and local governments, at times, imposing stay-at-home orders for their citizens. Unemployment has surged and economic recovery is uncertain. Many enterprises – especially those hardest hit in the hospitality industry – have experienced layoffs and budget cuts.

The pandemic and its shock to world economies have profoundly altered work environments and cybersecurity priorities. COVID-19 has prompted a massive work-from-home (WFH) movement, leading to the skyrocketing use of videoconferencing, collaboration tools, and cloud-based applications. Networks and remote access infrastructure have come under pressure. New threats have emerged targeting these technologies and pandemic-related anxieties. Meanwhile, many IT security teams are forced to do more with the same or fewer resources.

How has the COVID-19 pandemic specifically affected enterprise IT security organizations? How are they rethinking their priorities and investments? Well, thanks to the support of our research sponsors, we now have the answers we're looking for.

Top Five Insights for 2020

This report contains dozens of helpful insights on how COVID-19 has affected enterprise IT security teams. Here are our top five takeaways:

1. The 2020 budget shocker. Just when everyone thought that 2020 could finally be the year that IT security budgets stalled, we came along and are now dispelling that rumor. Our research indicates that the average enterprise IT security budget has received a 5% mid-year "boost" during the pandemic to fund additional remote access capacity, to secure personally owned devices accessing company applications and data, and to pretty much buy anything and everything that begins with the word "cloud."

2. Remote workforce tidal wave. Prior to the COVID-19 pandemic, about 24% of an enterprise's global workforce was working from home on a part-time or full-time basis. That number has risen to 50%, which equates to a 114% increase almost overnight. The implications of this so-called WFH movement are profound and, we believe, will influence the "new normal" for enterprises moving forward.

3. Spike in BYOD adoption. Before the pandemic, about 42% of enterprises employed bring-your-own-device (BYOD) policies that enable employees to use their home computers, smartphones, and tablets to access company applications and data. That number has spiked to 66%, equating to a 59% increase in a matter of months.

4. Not enough aspirin for these headaches. Every IT security team in every enterprise is feeling the effects of this global pandemic, including dealing with an increased volume of cyberthreats (37%), expanding insufficient remote access / VPN

SURVEY DEMOGRAPHICS

- **Responses received from 600 qualified IT security executives, managers, and practitioners**
- **All from organizations with 1,000 or more employees**
- **Representing seven countries: United States, Canada, United Kingdom, Germany, France, Australia, and Japan**
- **Representing 19 industries**

Introduction

capacity (35%), and mitigating increased risks stemming from unmanaged devices (35%). 73% of our respondents are also experiencing increases in third-party risks.

5. **A cloudy forecast.** Three in four (75%) IT security professionals now prefer cloud-based security solutions to traditional on-premises security solutions—and with good reason. This makes perfect sense as the top-three IT security technology investments made specifically to address new challenges stemming from the COVID-19 pandemic begin with the word, "cloud."

About This Report

The findings of this report are divided into four sections:

Section 1: Budgets & Personnel

A big unknown – especially to IT security vendors and service providers – is whether COVID-19 has negatively (or positively) affected IT security budgets this year and next year. Well, this survey report provides the answers – and the answers might surprise you. In this section, we also explore whether COVID-19 has introduced any new IT security staffing challenges, and if so, what are they.

Section 2: Work-from-home Movement

In this section, we assess the percentage of the typical enterprise workforce that worked from home before any of us knew what a coronavirus was versus the percentage of the workforce that is working from home today (or at least in August 2020 when this survey was conducted).

Then after touching on the potential expansion of bring-your-own-device (BYOD) policies, we gauge the appetite of IT security professionals who would like to work from once life returns to normal (post-vaccine, of course).

Section 3: IT Security Challenges

First, we explore what's keeping IT security professionals up at night during the pandemic. In other words, what new challenges are they facing while attempting to keep their employer's digital assets secure. Next, we'll assess how those respondents who are fortunate enough to have professional security certifications have fared during the pandemic. And finally, we'll evaluate the impact COVID-19 has had on third-party cybersecurity risks and programs.

Section 4: Technology Investments

In this last section, we learn what investments enterprises are making to address challenges faced due to the COVID-19 pandemic, including how enterprises are helping their work-from-home users secure their personally owned devices. We'll also validate or reject the notion that enterprises are turning to cloud-based security solutions in their time of need.

Navigating This Report

We encourage you to read this report from cover to cover so you don't miss any of the useful tidbits. However, there are three other ways to navigate through the report if you're looking for a particular topic:

- **Table of Contents.** Each topic in the Table of Contents pertains to a specific survey question. Click on any topic to jump to its corresponding page.
- **Research Highlights.** The Research Highlights page showcases the most significant headlines of the report. Page numbers are referenced with each highlight so you can quickly learn more.
- **Navigation tabs.** The tabs at the top of each page are clickable, enabling you to conveniently jump to different sections of the report.

Research Highlights

Budgets & Personnel

- **2020 budget shocker.** Just when everyone thought IT security budgets might get slashed, they actually went up mid-year – by an extra 5% (page 6).
- **2021 budget boost.** Next year's IT security budgets may set new records. Our respondents are hoping for a 7% budget increase next year (page 7).
- **Training and certification budget.** We're glad to see that enterprises won't be cutting back on training and certification next year. Budgets are anticipated to rise by a healthy 6% (page 8).
- **IT security skills shortage.** Most enterprise IT security teams were already short-handed before the pandemic, to the tune of 53% (page 9).
- **Staffing challenges.** Two-thirds (67%) of IT security teams experienced staffing challenges this year, including hiring freezes, furloughs, and layoffs (page 10).

Work-from-home Movement

- **Remote workforce tidal wave.** Today, half (50%) of enterprise employees are still working from home, an increase of 114% since the pandemic began (page 11).
- **Working without pants.** Four in five (81%) of IT security professionals are digging this work-from-home situation and want it to remain – at least a few days per week (page 12).
- **Spike in BYOD adoption.** The number of enterprises employing BYOD policies has risen 59% during the pandemic. Today, nearly two-thirds (66%) of enterprises allow personally owned devices to access company apps and data (page 14).

IT Security Challenges

- **Sleepless nights.** Every IT security team is facing new challenges, including increased cyberthreats (37%), insufficient remote access capacity (35%), and increased cyber risks (35%) (page 15).
- **Certifiably prepared.** Nearly four in five (78%) of those with IT security professional certifications feel better equipped to tackle pandemic-fueled security challenges (page 16).
- **Elevated third-party risks.** Nearly three in four (73%) enterprises have observed higher third-party risks (page 17).
- **Effects to third-party risk programs.** More than four in five (84%) of third-party risk management programs have been affected by the pandemic (page 18).
- **Working smarter through automation.** More than three in four (77%) IT security professionals agree that task automation is the key to solving elevated third-party risk challenges (page 19).

Technology Investments

- **Addressing pandemic challenges.** Cloud-based SWG (45%), cloud-based NGFW (43%), and cloud-based SEG (38%) are atop many shopping lists (page 20).
- **Mostly cloudy.** Three in four (75%) IT security professionals now prefer cloud-based security solutions to traditional on-prem offerings (page 21).
- **Securing personal devices.** Enterprises are investing smartly in technologies to secure personally owned devices, such as company-provided AV software (59%), MDM (52%), and NAC (48%) (page 23).

Section 1: Budgets & Personnel

Impact to 2020 IT Security Operating Budgets

How has COVID-19 affected your organization's 2020 IT security operating budget (e.g., products, services, personnel)?

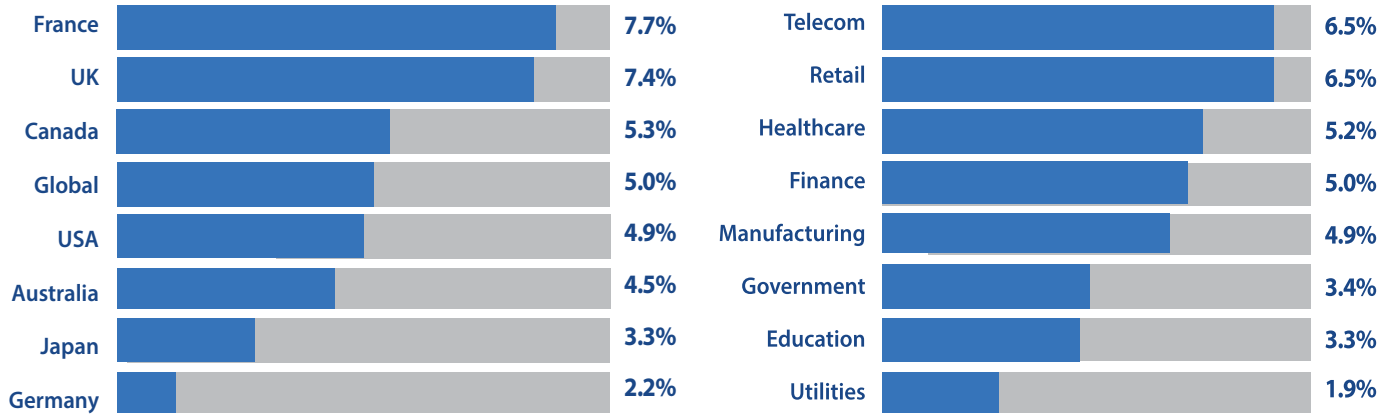

Figure 1: Mean mid-year increase to 2020 IT security operating budgets, by country and by industry.

There aren't enough fingers and toes to count on to describe the number of cybersecurity pundits who thought IT security budgets would be slashed in 2020 after the world went into lockdown last spring. And to be fair, several CyberEdge analysts are among them. But, boy, are we ever glad to be flat-out wrong!

Our first survey question out of the gate (after our demographic questions, of course) was to ask our IT security respondents how COVID-19 has affected their current 2020 operating budgets. We were pleasantly shocked to learn that the mean mid-year budget change is actually a 5% increase! Not the 5-10% decrease that so many of us were expecting. In total, 53.9% said their 2020 budgets are increasing, 19.7% said they're decreasing, and 26.4% said they're holding steady. All things considered, not too shabby!

Of course, the mean operating budget change varied among the countries and industries represented in our research study (see Figure 1), but not a single one of these groups had a mean budget decrease. France (+7.7%) and the telecom industry (+6.5%) are seeing the highest budget gains, while Germany (+2.2%) and the utilities industry (+1.9%) are seeing the lowest.

After the positive shock settled in for us, and after we breathed a huge sigh of relief, the mid-year budget increase started to make sense to us – especially after reviewing the immense operational challenges that IT security teams are facing, which we discuss later in this report (see page 15). The volume of cyberthreats are rising, cybersecurity risks are increasing, third-party risks are rising, and the remote workforce has more than doubled. There's no question that additional budget is needed to help put out these and other pandemic-fueled fires.

"We were pleasantly shocked to learn that the mean mid-year budget change is actually a 5% increase!"

Section 1: Budgets & Personnel

Impact to 2021 IT Security Operating Budgets

Do you expect your organization's overall IT security operating budget to increase or decrease in 2021?

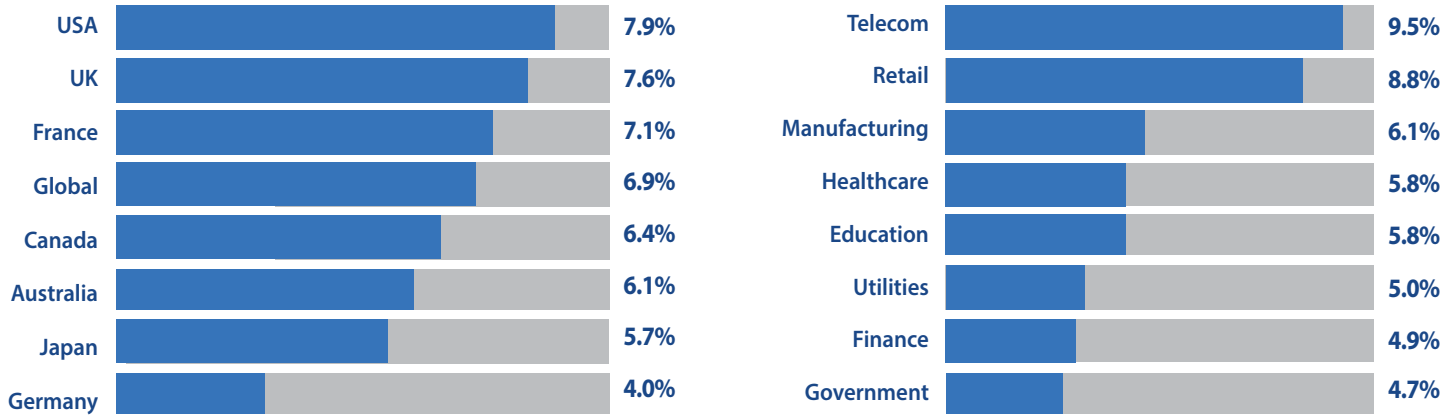

Figure 2: Mean anticipated increase to 2021 IT security operating budgets, by country and by industry.

To be fair, like most cybersecurity pundits, CyberEdge also suspected that 2021 could be the first year ever (at least that we're aware of) that IT security budgets might actually decline, or at least hold steady. Once again, we were pleasantly surprised and, frankly, relieved once we saw the results of this survey question.

After asking about the impact to current 2020 operating budgets (see prior section), we asked our respondents to predict how COVID-19 might affect next year's operating budget. We are thrilled to report a global mean anticipated budget increase of 6.9%. In total, 63.5% said they're expecting their operating budget to increase next year, 13.7% suspect it will decrease, and 22.8% think it will remain about the same.

Once again, next year's anticipated mean budget change varied by country and industry (see Figure 2). But just as before, not a single group's mean reflects an anticipated decrease for next year's operating budget. Respondents from the United States (+7.9%) and the Telecom (+9.5%) industry are the most bullish about next year's security budgets. Respondents from Germany (+4.0%) and the government (+4.7%) sector (across all seven countries – not just the United States) don't have quite as high expectations.

"In total, 63.5% said they're expecting their operating budget to increase next year."

For our readers who are also fans of CyberEdge's annual Cyberthreat Defense Report (CDR), you may recall that the mean anticipated IT security budget increases for "next year's budget" were +4.7% in 2018, +4.9% for 2019, and +5.0% for 2020. It's going to be interesting to see how COVID-19 impacts security operating budgets from the perspective of a broader audience (1,200 respondents from 17 countries) and organizations (500+ employees). We'll find out in April 2021 when the 2021 Cyberthreat Defense Report is published.

Section 1: Budgets & Personnel

Impact to 2021 IT Security Training & Certification Budgets

Do you expect your organization's IT security training and certification budget to increase or decrease in 2021?

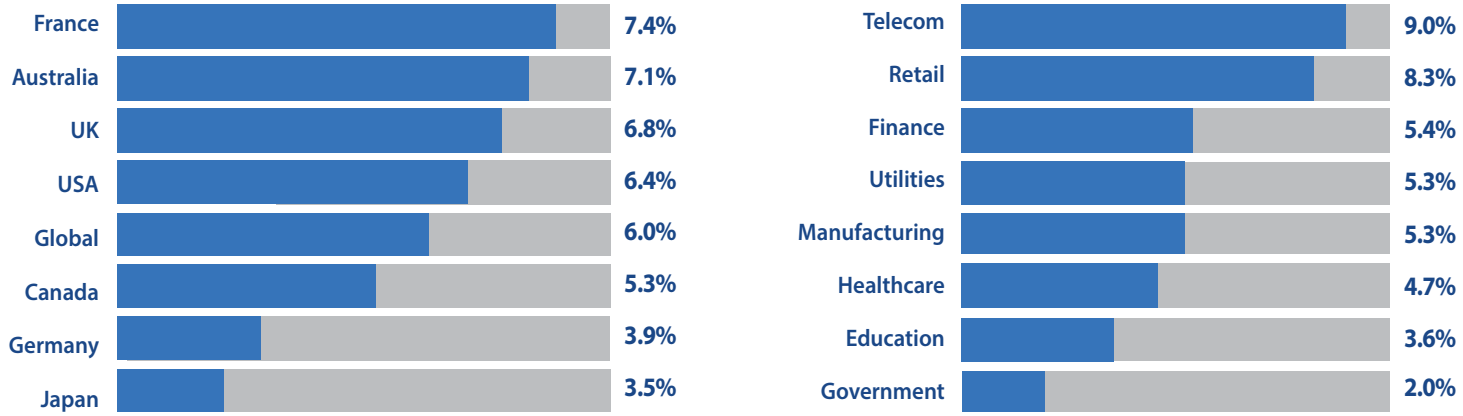

Figure 3: Mean anticipated increase to 2021 IT security training and certification budgets, by country and by industry.

CNBC.com published an article last year called, "Beyond a raise, this is what the majority of American workers want to be happier at work." CNBC and SurveyMonkey polled 8,664 professionals nationwide across all professions and industries. What do you think the number one response was for increasing workplace happiness? Yep, you guessed it – "more training or learning opportunities." Helping employees grow in their chosen professions is important.

We, at CyberEdge, know personally how incredibly impactful IT security training and certification truly is. (We touch on this topic again later in this report – see page 16). And we know from our 2020 Cyberthreat Defense Report that the number one motivation for achieving an IT security professional certification is "expanding knowledge of my chosen IT security profession." (The motivation at the bottom of the list was increased compensation.)

So, just as we were relieved to learn that 2020 operating budgets (on the whole) are still healthy, and that 2021 operating budgets are anticipated to rise, we were also pleased to see that enterprises are not cutting back on the IT security training and certification budgets. In fact, those budget allocations are anticipated to rise next year by an average of 6.0%, globally.

Delving into the data a little deeper, 61% of respondents anticipate a budget increase next year. This breaks down as follows: 54.0% expect a 1-10% increase; 28.2% expect an 11-20% increase; and 17.8% expect a 21% or more increase.

As always, results vary by country and industry (see Figure 3). Thankfully, all represented countries and industries indicate increased spending next year for IT security training and certification. France (+7.4%) and the telecom (+9.0%) industry reflect the highest anticipated budget increases (just as they do with mid-year 2020 budget increases). Japan (+3.5%) and government (+2.0%) organizations (again, across all seven countries) reflect the lowest anticipated budget increases.

Section 1: Budgets & Personnel

IT Security Personnel Shortage

Was your organization previously experiencing a shortage of skilled IT security personnel before the COVID-19 pandemic began?

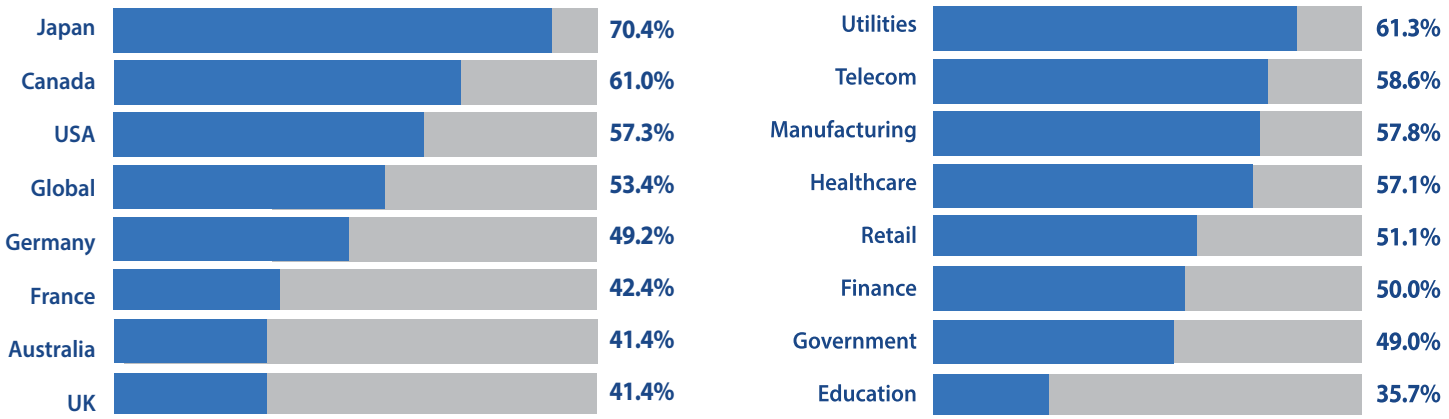

Figure 4: Enterprise experience a shortage of skilled IT security personnel, by country and by industry.

"We asked if organizations were experiencing a shortage of skilled IT security personnel before the pandemic began. A slight majority (53.4%) said that they were."

Every year for the past seven years, CyberEdge has asked IT security professionals who respond to our annual Cyberthreat Defense Report to rate (on a scale of 1 to 5) the potential barriers that might stand in their way from defending their employers' networks from cyberthreats. Guess what's consistently at or near the top of the list year-after-year. That's right… lack of skilled IT security personnel. (Great guess!)

In our COVID-19 survey, we asked our respondents if their organizations were experiencing a shortage of skilled IT security personnel before the pandemic began. A slight majority (53.4%) said that they were. The countries most affected (see Figure 4) are Japan (70.4%), Canada (61.0%), and the United States (57.3%). The industries most affected are utilities (61.3%), telecom (58.6%), and manufacturing (57.8%).

CyberEdge is a small research and marketing firm – not a large enterprise. So, it's hard for us to imagine what it's been like for you – our reader – to be tasked with securing your company's network with the exploding work-from-home movement, zillions of unmanaged devices accessing the network, and dramatically rising cyberthreat and third-party risks, all while you were under-staffed to begin with. Our hats are off to you.

Section 1: Budgets & Personnel

Workforce Spending Reduction Methods

Has your IT security organization experienced any of the following staffing challenges since the COVID-19 pandemic began?

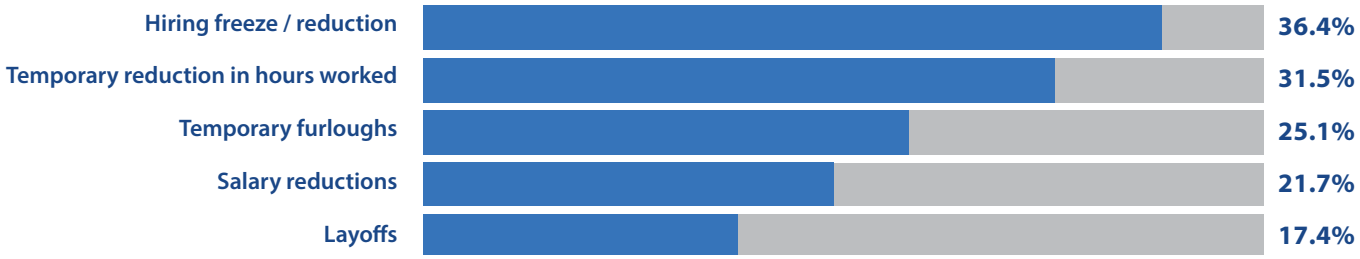

Figure 5: Workforce spending reduction methods used during the COVID-19 pandemic.

We hope you're not reading this report because you have extra time on your hands after being laid off or furloughed. If so, our hearts break for you. Despite an overall mid-year increase in 2020 IT security budgets, certainly not all organizations were that fortunate. In fact, about 20% of enterprises were forced to reduce their IT security operating budgets this year.

So, for enterprises with no other choice but to reduce their workforce spending, what were their most common workforce reduction methods pertaining to the IT security department? About one in three (36.4%) implemented a hiring freeze or cut back on their open headcount requisitions (see Figure 5). Next in line was temporarily reducing hours worked (31.5%), such as requiring employees to alternate work weeks – one week on, one week off (at half their salary).

The third most common tactic was temporary furloughs (25.1%), whereas employees were asked to stop working for a certain period of time or until further notice – without compensation, of course. Fourth was salary reductions (21.7%), requiring employees to do the same amount of work for less money – perhaps with the potential of reimbursing them later down the line. And finally, in fifth place, was layoffs (17.4%). Enough said there.

"This is the best possible time to recruit for new IT security personnel. You may never see such a large pool of qualified IT security candidates for the rest of your career. At least, let's hope so."

As finding and retaining skilled IT security talent is so challenging, it makes perfect sense that layoffs would be the last resort. And for organizations that aren't as adversely affected (such as those lucky IT security workers at Amazon.com, for example), this is the best possible time to recruit for new IT security personnel. You may never see such a large pool of qualified IT security candidates for the rest of your career. At least, let's hope so.

Section 2: Work-from-home Movement

Expanded Remote Workforce

What percentage of your organization's global workforce worked from home prior to the COVID-19 pandemic? And what percentage is still working from home today?

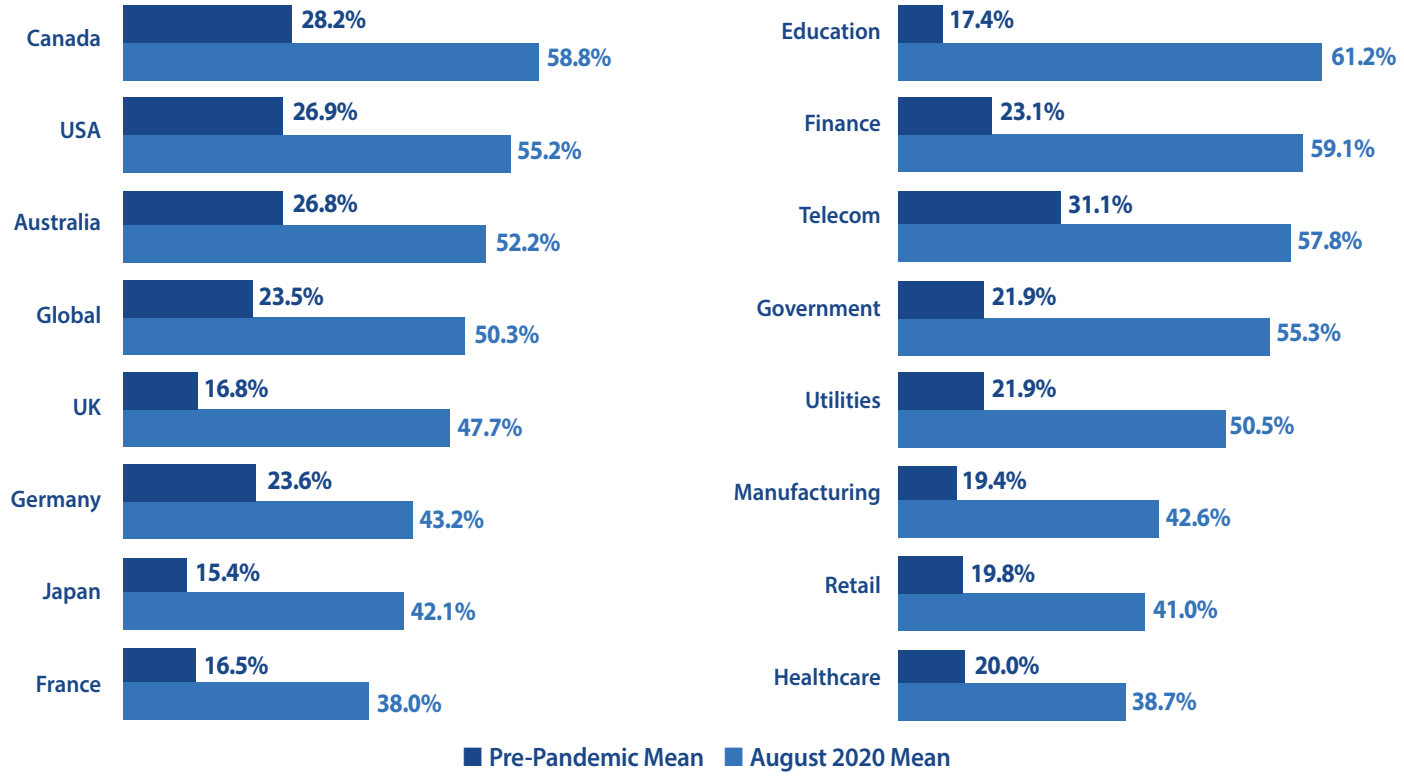

Figure 6: Percentage of global workforce working from home before and during the pandemic, by country and industry.

Arguably the biggest impact to IT security teams during this entire pandemic is the exploding work-from-home (WFH) movement. In a later section, we reference eight different challenges that IT security professionals have faced in recent months (see page 15) – in addition, of course, to the personal challenges of trying to conduct Zoom calls with small children running around.

Before we delve into the adverse effects of the pandemic, let's first try to assess how big of a deal this WFH movement really is. To do so, we asked our respondents to estimate the percentage of their employers' global workforce that was already working from home before the pandemic began versus "today" (which was in August 2020 when this survey was fielded).

Globally, the percentage of workers who worked from home (part-time or full-time) before the pandemic began was 23.5%. As of August 2020, that number was 50.3%, equating to a 114% increase in remote workers – all within a few months. Now, to be fair, we don't know if the 50.3% figure from August is the peak, or if perhaps that number was even larger in June and July, or if that figure will continue rising in September and October. Regardless, jumping from 23.5% to 50.3% is, indeed, a really big deal.

Of course, data varies by country and industry (see Figure 6). As of August 2020, Canada (58.8%) and the United States (55.2%) averaged the most remote workers, as did the education (61.2%) and finance (59.1%) industries.

Section 2: Work-from-home Movement

Work-from-home Preferences

After a COVID-19 vaccine becomes widely available and life returns back to normal, would you prefer to work from home or in the office?

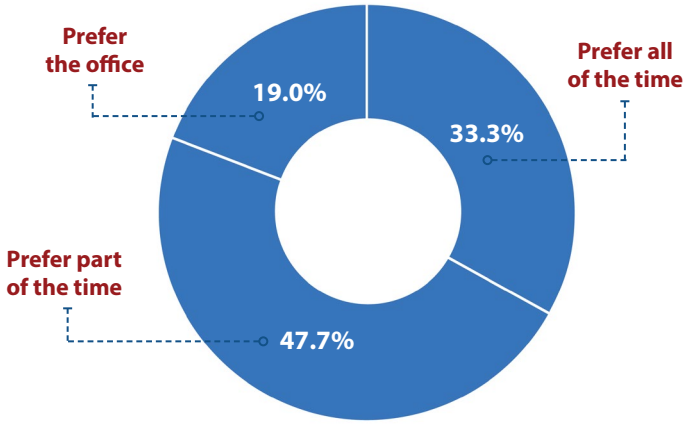

Figure 7: IT security professionals' preferences for working from home versus the office, globally.

Working from home is great. There's nothing like rolling out of bed, grabbing that first cup of morning joe, and getting right to work. But, to be fair, it's not for everyone.

Out of sheer curiosity, and to help out our IT security brothers and sisters who plan to ask their bosses if they can continue working from home once life returns to normal, we asked our respondents whether they'd prefer to work from home (part-time or full-time) or return back to the office. The results may surprise you (see Figure 7).

Four in five IT security professionals (81%) actually dig this work-from-home thing. It may have been challenging at first – especially for organizations who rely more heavily on on-premises equipment that must be maintained – but IT security professionals overwhelmingly want to work from home on a full-time (33.3%) or part-time (47.7%) basis.

With regard to preferences by country (see Figure 8), Germany (88.4%) and France (86.7%) top the list with the most IT security pros who aspire to work from home post-pandemic. Australia is simply down under (71.7%). (Sorry… had to.) By industry, telecom (87.8%) and utilities (86.5%) top that list, with retail (72.4%) at the bottom.

So, if you'd prefer to work from home after this pandemic has ended, fire up Zoom and show this report to your boss. Or if you're a people manager, take this statistic to heart and lobby the higher-ups for permission to continue this work-from-home culture beyond the pandemic. As previously discussed, the majority of IT security teams are short-staffed. It's challenging to hire and retain really good security people on a good day. So, seek out creative ways to use this statistic for your competitive advantage.

"Four in five IT security professionals (81%) actually dig this work-from-home thing."

Section 2: Work-from-home Movement

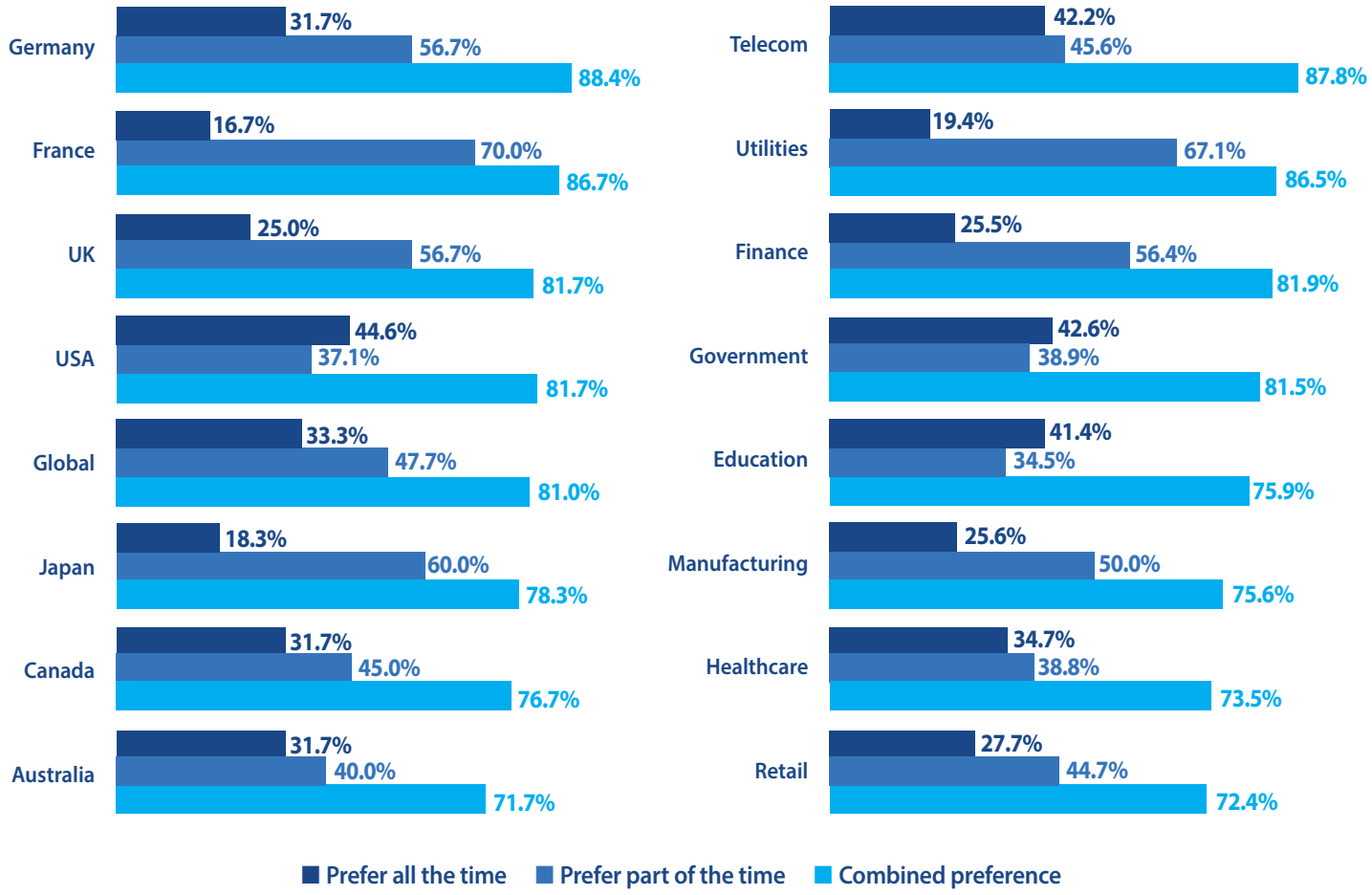

Figure 8: IT security professionals' preferences for working from home versus the office, by country and industry

Section 2: Work-from-home Movement

Increased BYOD Policy Adoptions

Does your organization have a BYOD (bring your own device) policy that permits employees to use personally owned devices to access company applications and data?

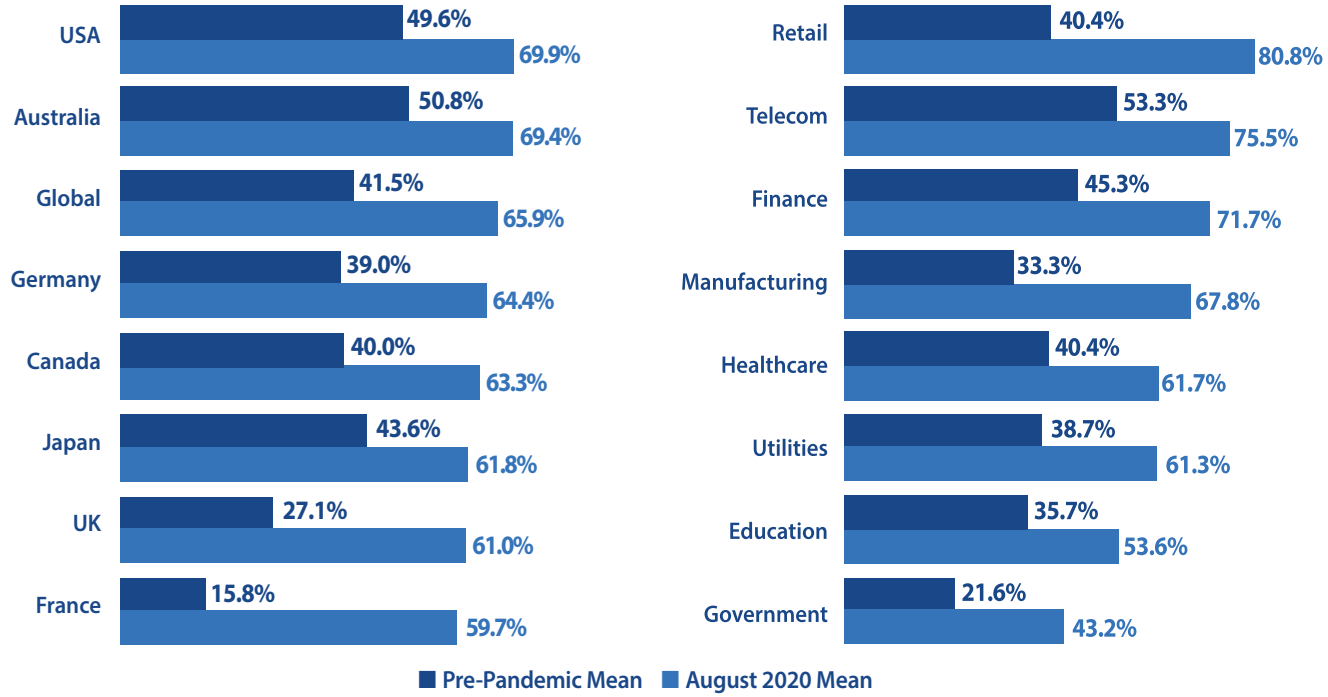

Figure 9: BYOD policy adoptions before versus during the COVID-19 pandemic, by country and by industry.

Before any of us knew what a coronavirus was, our respondents indicated that 41.5% of their employers already had a BYOD (bring your own device) policy in place, enabling employees to use their personal computers, tablets, and smartphones to access company applications and data. Since then, that number has risen from 41.5% to 65.9%. While the difference is only 24.4 percentage points, it actually equates to almost a 60% increase in only a few months.

This profoundly affects IT security teams that are suddenly thrown into the deep end of the proverbial BYOD swimming pool. And although a rise in BYOD adoption doesn't immediately affect companies who already had BYOD policies in place, this trend certainly affects their third-party cybersecurity risks, as many of their partners and suppliers are embracing BYOD for the very first time.

BYOD is both a blessing and a curse. On the positive side, it increases workforce productivity and improves morale. But BYOD dramatically increases cyber risks. Most employees outside the IT department know very little about properly securing personally owned endpoint devices.

Geographically speaking, the most significant rise in BYOD adoption (see Figure 9) occurred in France (278%), as it started out with the smallest percentage of BYOD deployments to begin with (only 15.8%). The country that currently has the highest percentage of enterprises with BYOD deployments is the United States (69.9%), closely followed by Australia (69.4%).

The industries which saw the biggest increases in BYOD adoption are government (100%) and retail (100%), which both doubled in size. The retail industry now boasts the highest BYOD adoption percentage (80.8%), followed by telecom (75.5%).

Section 3: IT Security Challenges

Operational Challenges

What have been the biggest challenges for your organization's IT security team during the COVID-19 pandemic? Select all that apply.

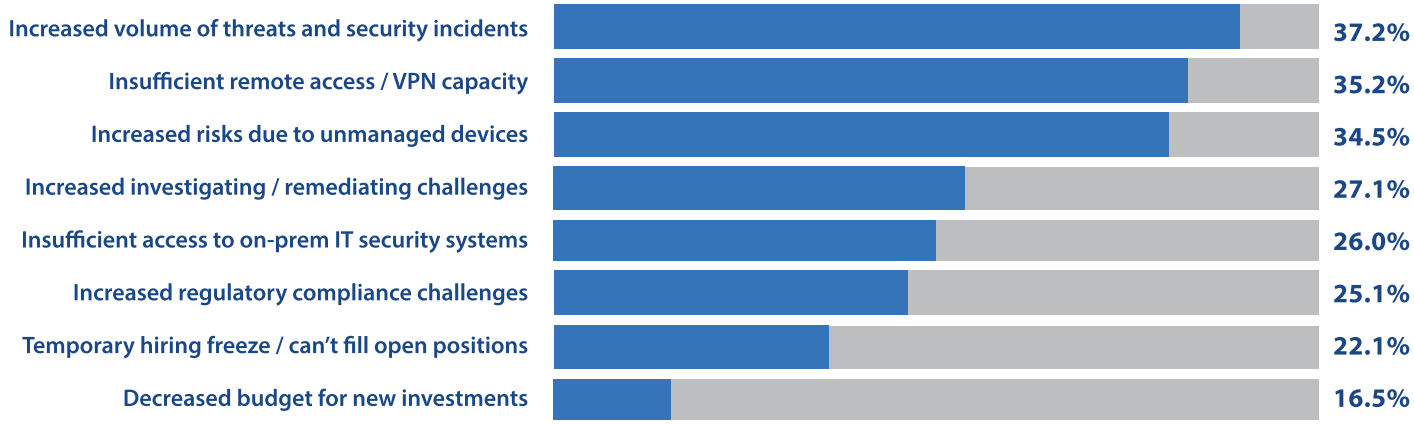

Figure 10: IT security operational challenges stemming from the COVID-19 pandemic.

It's hard for people outside the IT security department to understand the enormous impact that the COVID-19 pandemic has had on our profession. Can you imagine being a CSO of a major enterprise? How much sleep could they be getting? Waking up to nightmares of TV news anchors speaking their company's name followed by the words, "data breach." How stressful.

Of course, virtually all IT security professionals have been, and still are, under an incredible amount of stress. So, we wanted to find out what specific challenges enterprise IT security teams are facing (see Figure 10) as a result of this pandemic. No huge surprises here, except for the pleasant surprise at the bottom of the chart above. Let's get into it.

First, 37.2% of organizations are seeing an increased volume of threats and security incidents. There have been numerous reports of COVID-19-specific phishing and spear-phishing attacks, remote desktop protocol (RDP) attacks, ransomware attacks, brute-force attacks, and who knew we'd be talking about "Zoom bombing!" In second position, insufficient remote access / VPN capacity (35.2%), which naturally includes ensuring there's enough bandwidth available to connect everyone back to HQ! And third, increased risks due to unmanaged devices (34.5%), which stems, of course, from the 60% overall increase in BYOD adoption.

"It's hard for people outside the IT security department to understand the enormous impact that the COVID-19 pandemic has had on our profession."

At the bottom of the list, for which we're all very grateful, is decreased budget for new investments (16.5%). As we discussed right out of the gate, the average mid-year change in 2020 IT security budgets is a 5% increase. Thankfully, this challenge only affected about one in six enterprise security teams.

Section 3: IT Security Challenges

Professional Certification Preparedness

Describe your agreement with the following statement: "My IT security professional certification has better equipped me to meet the challenges our IT security team has faced since the pandemic began."

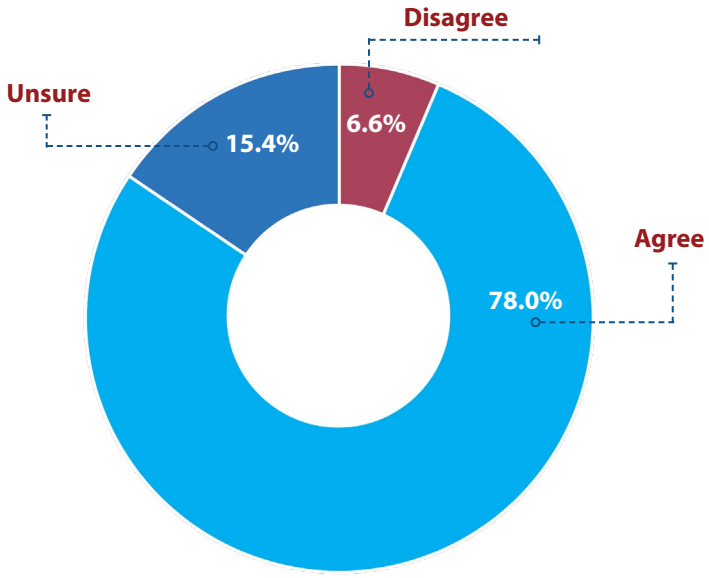

Figure 11: Respondents who feel their professional certifications made them better prepared to meet pandemic challenges.

"So, if you're trying to move up the ladder and don't have a professional certification, it could be one of the factors that's holding you back."

There's an interesting statistic from CyberEdge's 2020 Cyberthreat Defense Report that is particularly relevant to this next topic. We asked security professionals with professional certifications to rate the benefits they experience as a result of achieving their respective certifications. At the bottom of the list was increased compensation. At the top of the list was expanding knowledge of their chosen IT security profession. In other words, it's not about the Benjamins! (Okay, it's a little about the money. But that's not the driving factor.)

Extending this topic to this COVID-19 study, we asked our respondents with IT security professional certifications to confirm whether their certification has better equipped them to meet the challenges faced during the pandemic (see Figure 11). Not surprising, nearly four in five (78%) agreed, which aligns perfectly with the aforementioned Cyberthreat Defense Report insight. Only 6.6% disagreed (perhaps those are our money grubbers). 15.4% were unsure, which is reasonable because not all IT security roles are affected the same from the WFH movement and increased BYOD policy adoption.

In case you're curious what percentage of our respondents had already achieved one or more IT security certifications, that number would be 90.8%. (The stats in Figure 11 are only derived from these people.) So, if you're trying to move up the ladder and don't have a professional certification, it could be one of the factors that's holding you back.

Section 3: IT Security Challenges

Impact to Third-Party Risks

With so many organizations embracing the work-from-home movement, how has the pandemic affected your company's cyber risks associated with third parties?

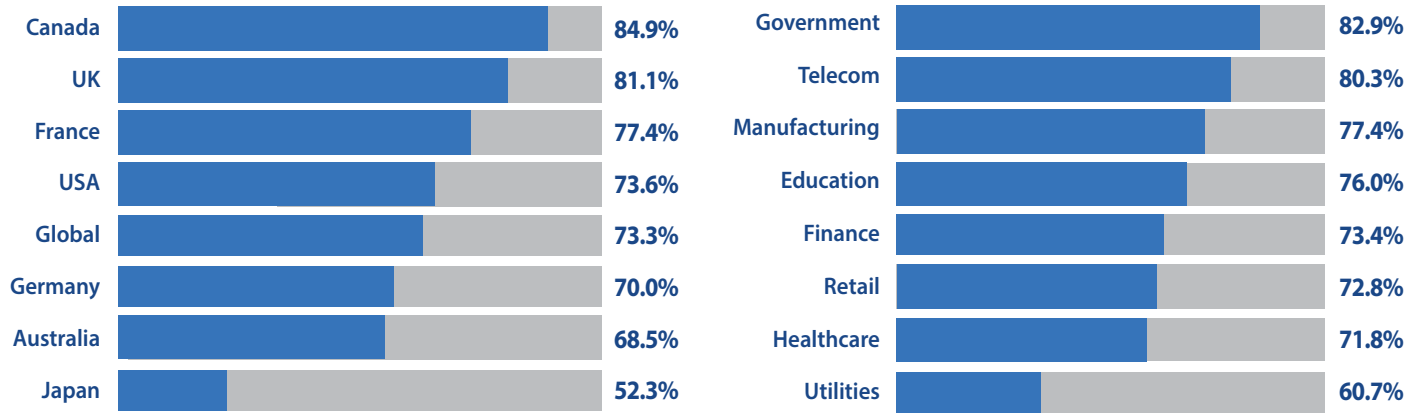

Figure 12: Enterprises experiencing higher third-party risks during the COVID-19 pandemic, by country and industry.

"Globally, nearly three in four (73.3%) enterprises have experienced elevated third-party risks."

Running an effective third-party risk management (TPRM) program is a critical function of every enterprise IT security organization. Assessing the security posture of your partners and suppliers is paramount. A major data breach or disruption of service of a strategic partner or supplier can have devastating consequences to your company. Thus, smart security executives rely on cybersecurity ratings vendors to continuously monitor the cyber resilience of their strategic partners.

As we've discussed throughout this report, the COVID-19 pandemic has caused an instantaneous doubling of a typical remote workforce. And we already know that BYOD policy adoption has skyrocketed this year, causing significant increases in the volume and severity of cyberthreats. This not only adversely affects your organization, but your strategic partners and suppliers, as well.

So, how has the pandemic affected third-party risks? Well, we now have the answers (see Figure 12). Globally, nearly three in four (73.3%) enterprises have experienced elevated third-party risks. Enterprises in Canada (84.9%) are feeling the worst of it, while Japanese enterprises (52.3%) are less affected. Enterprises in the government (82.9%) sector are certainly feeling the pain, while utilities (60.7%) are not as affected.

With third-party cyber risks at an all-time high, how has this affected enterprise TPRM programs? You'll find the answer to that question on the next page.

Section 3: IT Security Challenges

Impact to Third-Party Risk Management Programs

How has the pandemic affected your organization's third-party cybersecurity risk management program? Select all that apply.

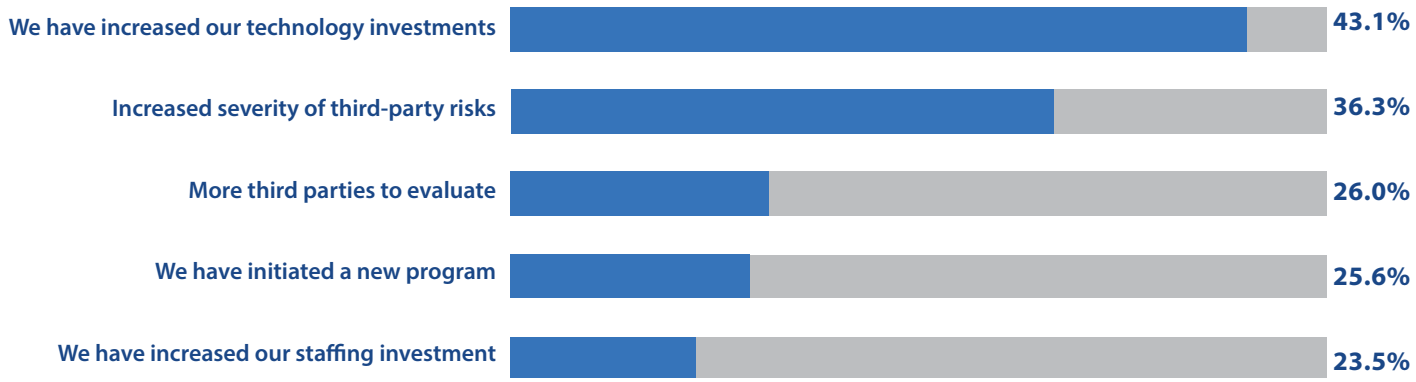

Figure 13: Pandemic effects on third-party risk management programs.

Now that we've established that 73.3% of enterprises are seeing an increased volume of third-party cyber risks (see Figure 12 on page 17), let's discuss how this has impacted enterprise third-party risk management (TPRM) programs.

We asked our respondents to select among five TPRM likely outcomes (see Figure 13). The most widely selected outcome was increasing technology investment (43.1%). Prior to the pandemic, and even still today, it's surprising how many enterprises conduct third-party cyber risk assessments internally using spreadsheets, questionnaires, or other rudimentary methods that give you a snapshot of third-party risk at a moment in time. Given the mid-year influx of expanded IT security funding (for most enterprises, at least), many IT security teams spent wisely and contracted with cybersecurity ratings vendors so they can continuously monitor cyber risks associated with their most-strategic partners and suppliers.

The second highest-rated outcome is increased severity of third-party risks (36.3%). So, not only are enterprises seeing an increased volume of third-party risks, but they're also experiencing increased severity, as well. Oh, goodie. The bottom three outcomes are more third parties to evaluate (26.0%), initiating a new TPRM program (25.6%), and increasing staffing investment (23.5%). So nice to be able to actually hire someone during this global crisis.

There's one more comforting tidbit of information that was yielded from this survey question. Globally, 94.3% of enterprises now have a formal TPRM program. If your company is one of the 5.7% that doesn't have one, then take this survey report directly to your CSO and demand that a new TPRM program is created. Or, if making career-limiting moves is not your thing, when you're back in the office print out this report, earmark this page, highlight the aforementioned statistic, and anonymously leave the report on your CSO's desk. That works, too.

Section 3: IT Security Challenges

Third-Party Risk Management Automation

Describe your agreement with the following statement: "Automating key tasks (e.g., reporting, risk prioritization) within our third-party risk management tools/platform would enable us to do more with fewer resources."

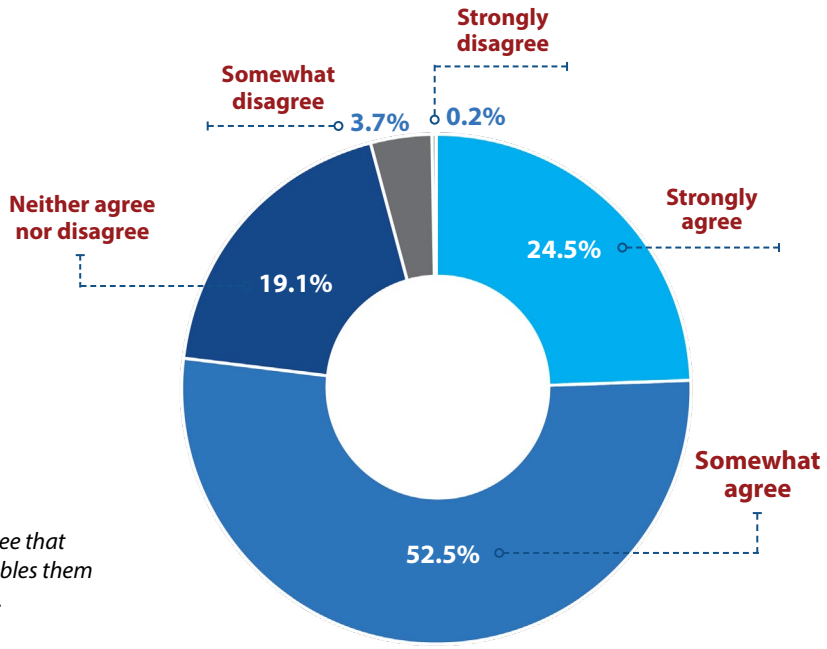

Figure 14: Respondents who agree that automating key TPRM tasks enables them to do more with fewer resources.

The third survey question of our third-party risk management (TPRM) trifecta is about automation. Specifically, it's about validating the positive impact that automating key TPRM tasks brings to enterprise IT security teams.

"When you're already spread so thin, it's important to embrace technology that enables you to work smarter – not harder."

We asked our respondents whether they agree or disagree that automating key tasks – such as third-party risk reporting and risk prioritization – would enable their IT security organization to do more with fewer resources. As you might expect, just over three in four (77%) respondents agreed with this statement (see Figure 14).

As we learned earlier in this report, 53.4% of enterprises are experiencing a shortage of skilled IT security personnel. (It's even higher when you expand the survey base to small-to-medium size enterprises, as we do each year in our Cyberthreat Defense Report.) When you and your colleagues are already spread so thin, it's important to embrace technology that enables you to work smarter – not harder – as there are only so many hours in the day.

For those of you evaluating third-party cybersecurity risk ratings vendors, don't just consider the quality of their data, but inquire about how their solution can save you time and effort through task automation. You'll thank us later.

Section 4: Technology Investments

Pandemic-fueled Technology Investments

Which of the following technologies were acquired this year, or are in the process of being acquired, specifically to address new challenges stemming from COVID-19? Select all that apply.

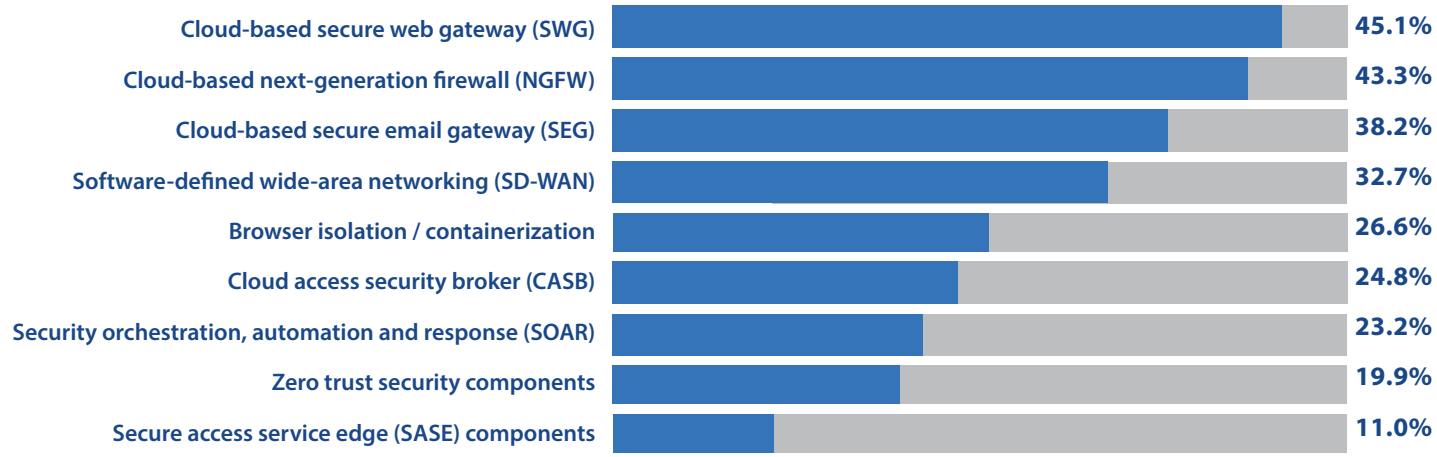

Figure 15: Security technologies that address new challenges stemming from the COVID-19 pandemic.

As we head down the home stretch of this survey report, we've got three more sets of results to review – all pertaining to technology investments.

Here, we asked our respondents to identify which technologies their organizations are investing in that will help address new challenges stemming from the COVID-19 pandemic (see Figure 15). The top-three all share something in common: cloud-based secure web gateway (45.1%), cloud-based next-generation firewall (43.3%), and cloud-based secure email gateway (38.2%). These 'must-have' security technologies originally started out as on-prem appliances, but lately more enterprises have been embracing cloud-based alternatives for a variety of valid reasons. We'll leave it at that, for now, as we don't want to steal any thunder from the next section.

The remaining technology investments are fueled by the COVID-19 pandemic in different ways:

- SD-WANs (32.7%) help connect remote workers in a way that is more cost-effective, secure, and higher-performing than traditional MPLS-based VPNs.
- Browser isolation (26.6%) enables users with unmanaged devices (think BYOD) to execute content within the safety of cloud-based virtual machines, helping to mitigate risks associated with malware, ransomware, and other cyberthreats.
- CASBs (24.8%) help mitigate risks associated with Shadow IT, protect against malware, prevent data leakage, and help govern usage of SaaS-based applications.
- SOAR (23.2%) help IT security teams do more with fewer resources by automating key security tasks and orchestrating workflows.
- Zero trust security (19.9%) is an alternative to traditional VPNs that provides remote users with direct, secure access to any application, regardless of where it resides.
- SASE (11.0%) converges WAN and network security services (e.g., IPS, NGFW, CASB, SWG) into a unified, cloud-native service, giving remote users the secure access they need while making life simpler for IT security administrators who also work from home.

Section 4: Technology Investments

Preference for Cloud-based Security Solutions

How has COVID-19 affected your organization's preference for selecting and deploying cloud-based (i.e., SaaS) versus on-premises IT security solutions?

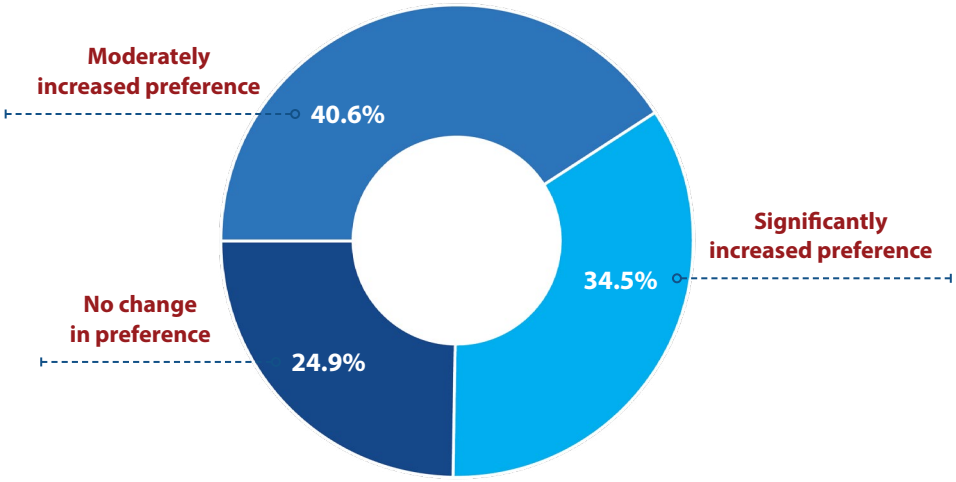

Figure 16: Enterprise IT security team preferences for cloud-based security solutions.

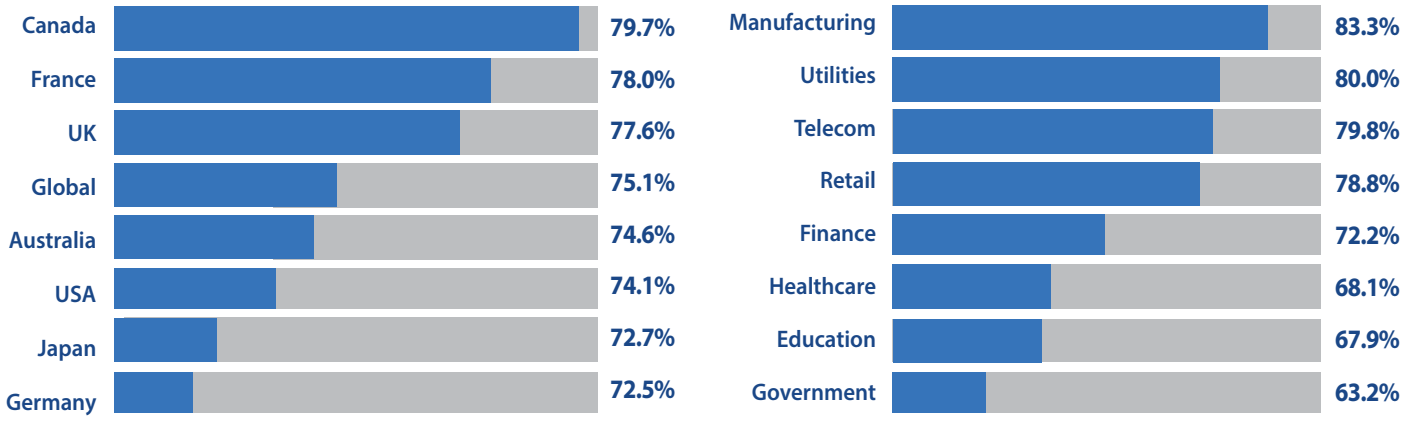

Figure 17: Preferences for cloud-based security solutions, by country and industry.

Since the COVID-19 pandemic began, there's been an awful lot of hype from security vendors claiming that COVID-19 is fueling expanded investment in cloud-based security technologies. Are they right? Or is this just marketing hype?

Well, it turns out that they're exactly 75.1% correct (see Figure 16), at least according to our survey. Three-quarters of our respondents have indicated a significant increase (34.5%) or moderate increase (40.6%) in preference for security solutions

Section 4: Technology Investments

delivered via the cloud. And, honestly, it makes perfect sense as half the typical enterprise workforce is working remotely these days, which also includes a heck of a lot of IT security professionals. There simply aren't enough people on site to administer on-prem servers and appliances. But even if all members of the IT security team were back in the office, there's still so many benefits to cloud-based security solutions, including cost, performance, and scalability. Let's face it. The security world is very cloudy these days, which is a great thing.

Now, preferences for cloud-based security solutions doesn't vary much by country (see Figure 17), ranging from 72.5% (Germany) to 79.7% (Canada). But preferences do vary a bit more by industry, with manufacturing (83.3%) as the most pro-cloud and government (63.2%) as the least. The latter makes sense as it's probably not the best idea to store top-secret plans for your next-generation stealth fighter on a public file sharing site.

"Three-quarters of our respondents have indicated a significant increase (34.5%) or moderate increase (40.6%) in preference for security solutions delivered via the cloud."

Section 4: Technology Investments

Securing Personally Owned Devices

Which of the following technologies does your organization use to help secure personally owned devices? Select all that apply.

Figure 18: Security technologies used to help secure personally owned devices accessing corporate apps and data.

Earlier in this survey report, we learned that nearly two-thirds (65.9%) of enterprises have implemented bring-your-own-device (BYOD) policies – many of which did so just within the past 6-9 months. As few employees outside the IT security department know how to properly secure their endpoint devices (e.g., home computers, tablets, and smartphones), enterprises have recently been investing in technologies to help mitigate the cyber risks that BYOD imposes.

Specifically, there are five technologies that help to secure personally owned devices used to access corporate applications and data:

- Company-provided AV / anti-malware software (59%) is an endpoint security staple. Recent advancements in machine learning (ML) and artificial intelligence (AI) are helping to defend against modern threats missed by traditional signature-based AV.
- Mobile device management (MDM; 52.1%) helps enforce device-level security policies with regard to identity management, password requirements, and patching on smartphones and tablets.
- Network access control (NAC; 48.2%) restricts access to corporate resources to only those devices that meet certain security standards, such as the presence of AV software, up-to-date AV signatures, and up-to-date operating system and application patches.
- Mobile application management (MAM; 43.7%) allows IT security to apply and enforce corporate policies to company applications running on smartphones and tablets.
- Browser isolation (32.9%) enables users to execute content within the safety of cloud-based virtual machines. Any malware contained within that content vanishes the moment the user stops accessing that content.

Conclusion

The COVID-19 pandemic has turned so much of our world upside down, both personally and professionally. Enterprise IT security teams have had to cope with so many challenges this year:

- 114% increase in employees working from home
- 59% increase in BYOD policies
- 53% of enterprises experiencing a shortage of skilled IT security personnel
- 36% of enterprises implementing a hiring freeze and/or future headcount reduction
- Increased volume of threats and security incidents
- Increased third-party cyber risks in volume and severity
- Insufficient remote access / VPN capacity

But the news isn't all bad. Survey respondents also indicated several positives:

- Average of a 5% mid-year budget increase to fund new security investments
- Projected 7% IT security budget increase for 2021
- Projected 6% security training and certification budget increase for 2021
- 94% of organizations have a third-party risk management (TPRM) program in place
- 43% are investing more in TPRM technologies, especially those with task automation
- MDM, MAM, NAC, and browser isolation are helping to secure unmanaged devices
- Enterprises are evolving from an on-prem mentality to a cloud state of mind
- Those with IT security professional certifications are feeling particularly prepared
- Hope for 80% of you, when life returns to normal, that you might still be allowed to work from home and attend virtual meetings without wearing pants (or "trousers" for our friends outside the U.S.)

So, what can we learn from all these positives and negatives? We have a few thoughts to share.

Reducing work-from-home risks is priority one.

If your remote workforce is using personally owned computers and devices to access your company's applications and data, and those devices still haven't been effectively secured, then securing those endpoints should be your number one priority. Embrace those technologies (e.g., MDM, MAM, NAC, and browser isolation) that can help reduce the collective attack surface of these unmanaged devices.

Adopt a cloud mentality.

For those of you who can remember the exact sound that your dial-up modem made when it connected to Prodigy or America Online in the 1980s, it's time to shift your thinking away from legacy on-prem appliances toward cloud-based security solutions (at least when the option to choose presents itself). There are just too many good reasons to embrace modern cloud security offerings – especially with supporting a distributed workforce.

Formal IT security training and certification makes a huge difference.

Conclusion

Keep a close eye on third-party cyber risks.

You can increase your IT security operating budget, you can embrace every best practice, you can hire the very best people… hell, you could wave a magic wand and make all of your company's internal cyber risks disappear… and your company would still be at risk because your strategic partners and suppliers haven't done the same. While it's great that 19 in 20 enterprises have TPRM programs in place, it doesn't mean that you've done enough due diligence by reassessing third-party cyber risks. No more spreadsheets. No more questionnaires. Invest in cybersecurity ratings vendors that continuously monitor the cyber resilience of your strategic partners and suppliers

Formal IT security training and certification makes a huge difference.

From this COVID-19 study, we learned that 78% of IT security employees with formal training and certification feel better equipped to deal with the challenges stemming from this pandemic. And we also know from our 2020 Cyberthreat Defense Report that the number one motivation for achieving an IT security professional certification is "expanding knowledge of my chosen IT security profession." So, invest in your people. And help close your IT security hiring gap by using the promise of training and certification as a recruiting incentive.

In closing, there's an oft misunderstood proverb that reads, "May you live in interesting times." It's an English expression that purports to be a translation of a traditional Chinese curse, as life is usually better in uninteresting times of peace and tranquility. This proverb is particular fitting today as we're definitely living in interesting times, COVID-19 originated from China, and we're all feeling a little "cursed" right now. But rest assured, there are blue skies ahead. We'll get through this pandemic together.

Until a vaccine is developed, and life returns to a "new normal," we at CyberEdge hope that you and your family live in safe times.

Survey Demographics

This report is based on web-based survey responses from 600 qualified participants from seven countries (see Figure 19).

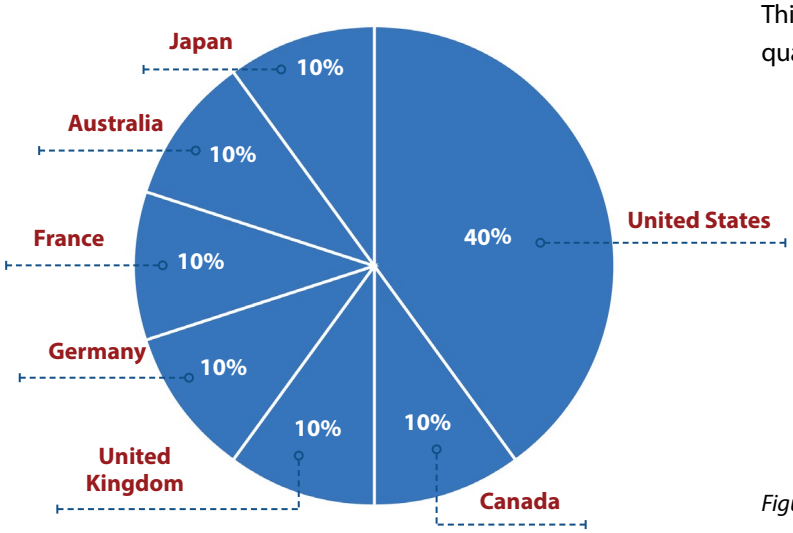

Figure 19: Survey respondents by country.

Each respondent was required to have a role in their employer's IT security department (see Figure 20).

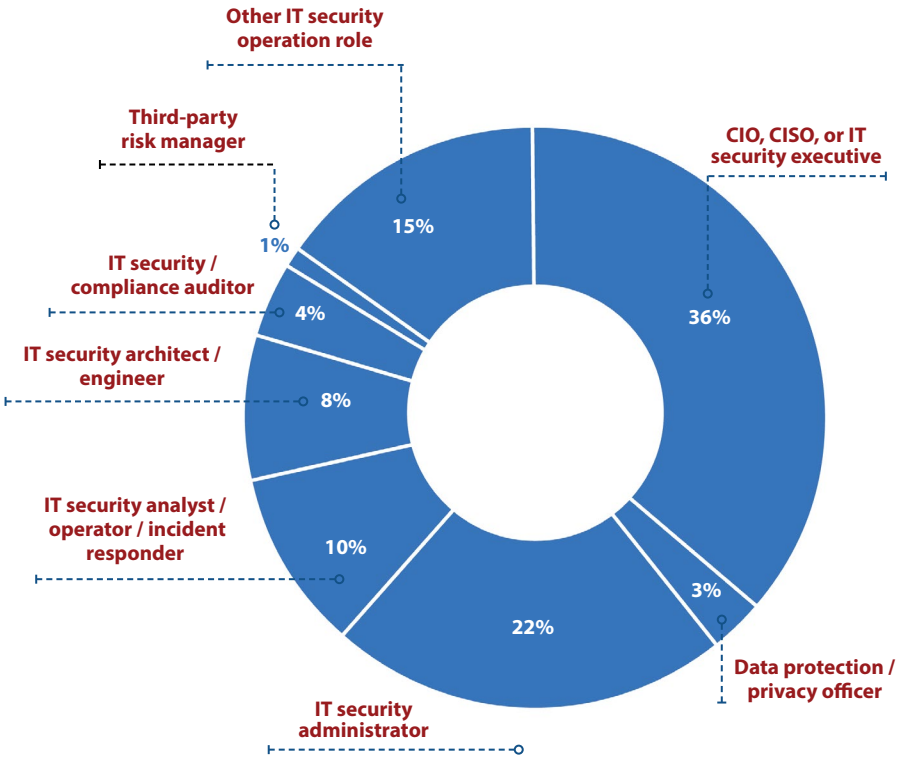

Figure 20: Survey respondents by IT security operations role.

Survey Demographics

All participants in this survey were working for enterprises with 1,000 or more employees (see Figure 21). They spanned 19 industries (plus "Other") with no single industry having more than 15% of the total participants. For selected questions, additional analysis was conducted based on the eight industries with the largest percentage of respondents (see Figure 22). Those eight industries—telecom, manufacturing, finance, government, healthcare, retail, utilities, and education—collectively comprise almost 85% of the research participants.

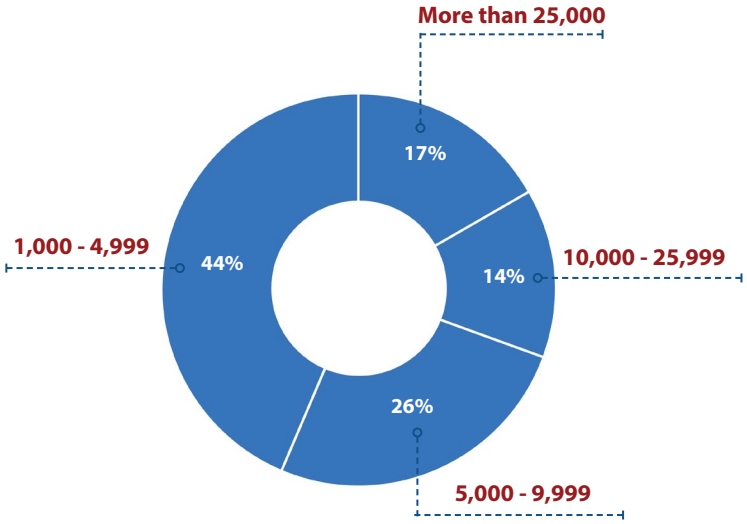

Figure 21: Survey respondents by organization employee count.

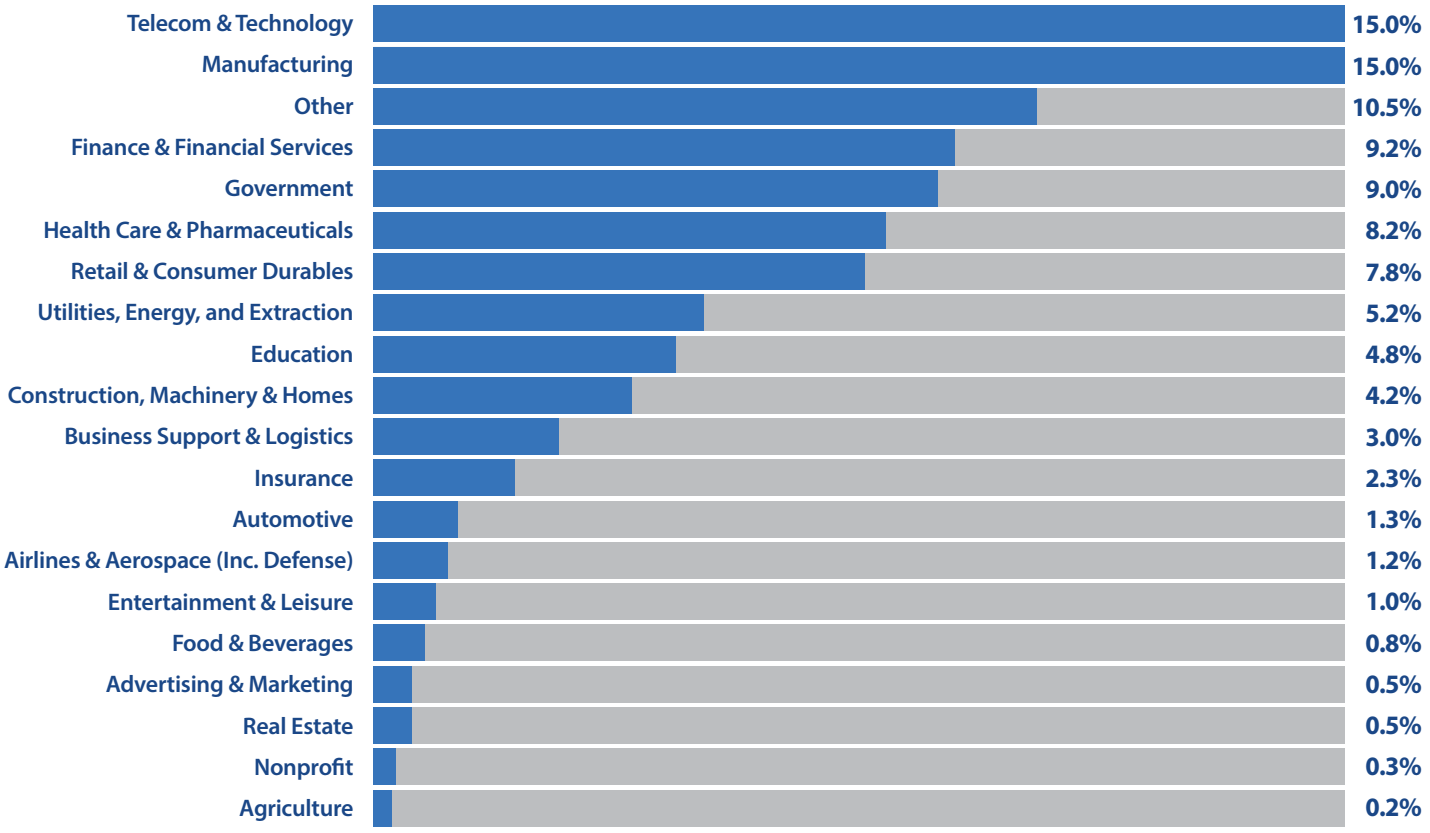

Figure 22: Survey respondents by industry.

Research Methodology

CyberEdge developed a 20-question web-based, vendor-agnostic survey instrument in partnership with our research sponsors. The survey was promoted via email to 600 IT security professionals in the United States, Canada, United Kingdom, Germany, France, Australia, and Japan in August 2020. The global survey margin of error for this research study (at a standard 95% confidence level) is 5%. All results pertaining to individual countries and industries should be viewed as "anecdotal" as their sample sizes are much smaller. CyberEdge recommends making actionable decisions based on global data only.

All respondents must meet two filter criteria: (1) they must have an IT security role and (2) they must be employed by a commercial or government organization with a minimum of 1,000 global employees.

At CyberEdge, survey data quality is paramount. CyberEdge goes through extraordinary lengths to ensure its survey data is of the highest caliber by following these industry best practices:

- Ensuring that the "right" people are being surveyed by (politely) exiting respondents from the survey who don't meet the respondent filter criteria of the survey (e.g., job role, job seniority, company size, industry)
- Ensuring that disqualified respondents (who do not meet respondent filter criteria) cannot restart the survey (from the same IP address) in an attempt to obtain the survey incentive
- Constructing survey questions in a way to eliminate survey bias and minimize the potential for survey fatigue
- Only accepting completed surveys after the respondent has provided answers to all of the survey questions
- Ensuring that survey respondents view the survey in their native language (e.g., English, German, French, Spanish, Japanese, Chinese)
- Randomizing survey responses, when possible, to prevent order bias
- Adding "Don't know" (or comparable) responses, when possible, so respondents aren't forced to guess at questions they don't know the answer to
- Eliminating responses from "speeders" who complete the survey in a fraction of the median completion time
- Eliminating responses from "cheaters" who apply consistent patterns to their responses (e.g., A,A,A,A and A,B,C,D,A,B,C,D)
- Ensuring the online survey is fully tested and easy-to-use on computers, tablets, and smartphones

CyberEdge would like to thank our research sponsors for making this survey report possible and for sharing their IT security knowledge and perspectives with us.

About Our Sponsors

(ISC)² | www.isc2.org

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, pragmatic approach to security. Our membership, more than 150,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the general public through our charitable foundation – The Center for Cyber Safety and Education™.

Gigamon | www.gigamon.com

Gigamon is the first company to deliver unified network visibility and analytics on all data-in-transit, from raw packets to apps, across physical, virtual and cloud infrastructure. We aggregate, transform and analyze network traffic to solve for critical performance and security needs, including rapid threat detection and response, freeing your organization to drive digital innovation. In short, we enable you to run fast, stay secure and innovate.

SecurityScorecard | www.securityscorecard.com

SecurityScorecard is the global leader in cybersecurity ratings and the only service with over a million companies continuously rated. Founded in 2013 by security and risk experts, Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 1,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, and cyber insurance underwriting. SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors.

Thycotic | www.thycotic.com

The easiest to manage and most readily adopted privilege management solutions are powered by Thycotic. Thycotic's security tools empower over 10,000 organizations, from small businesses to the Fortune 500, to limit privileged account risk, implement least privilege policies, control applications, and demonstrate compliance. Thycotic makes enterprise-level privilege management accessible for everyone by eliminating dependency on overly complex security tools and prioritizing productivity, flexibility, and control. Headquartered in Washington, DC, Thycotic operates worldwide with offices in the UK and Australia.

About CyberEdge Group

Founded in 2012, CyberEdge is the largest research, marketing, and publishing firm to serve the IT security vendor community. Today, approximately one in seven established IT security vendors (with $10 million or more in annual revenue) is a CyberEdge client.

CyberEdge's highly acclaimed Cyberthreat Defense Report (CDR) and other single- and multi-sponsor survey reports have garnered numerous awards and have been featured by both business and technology publications alike, including The Wall Street Journal, Forbes, Fortune, USA Today, NBC News, ABC News, SC Magazine, DarkReading, CISO Magazine, and others.

CyberEdge has cultivated its reputation for delivering the highest-quality survey reports, analyst reports, white papers, and custom books and eBooks in the IT security industry. To learn more about how we help our IT security vendor clients succeed, connect to our website at www.cyber-edge.com.

CYBEREDGE GROUP

CYBEREDGE GROUP, LLC

1997 ANNAPOLIS EXCHANGE PKWY.
SUITE 300
ANNAPOLIS, MD 21401

800.327.8711

WWW.CYBER-EDGE.COM

INFO@CYBER-EDGE.COM