• 10 IN 10 STUDY •

THE INDELIBLE IMPACT OF COVID-19 ON CYBERSECURITY

Bitdefender®

WWW.BITDEFENDER.COM

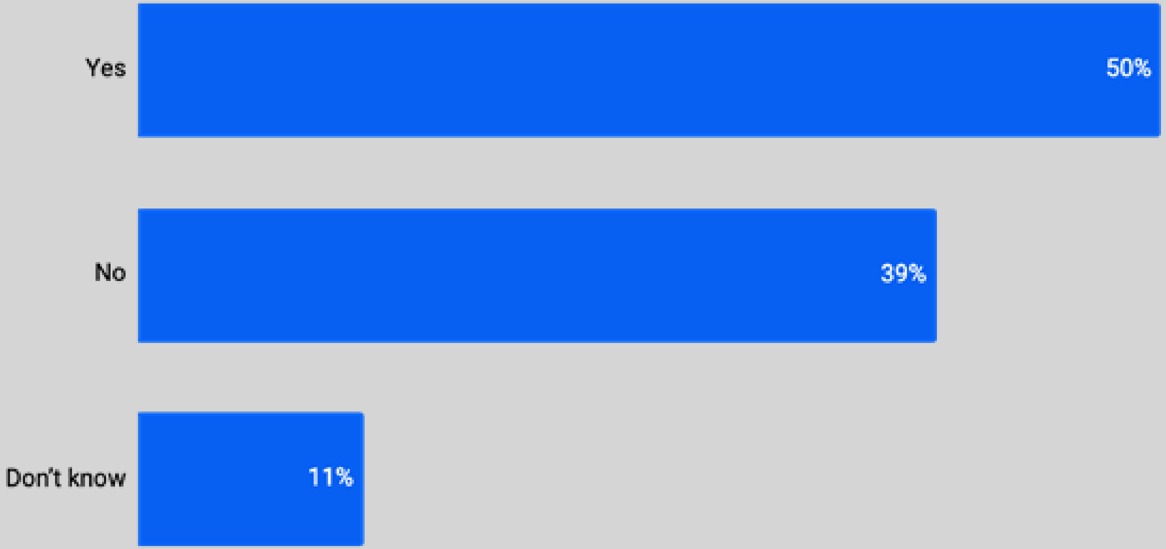
ACCORDING TO INFOSEC PROFESSIONALS

- ○ 50% HAD NO CONTINGENCY PLAN IN PLACE FOR COVID-19
- ○ 86% ADMITTED THAT ATTACKS WERE ON THE RISE DURING THIS PERIOD
- ○ 81% BELIEVE THAT COVID-19 WILL CHANGE THE WAY THEIR BUSINESSES OPERATE LONG-TERM
- ○ PHISHING/WHALING ATTACKS WERE THE MOST COMMON TYPE OF ATTACK TO SEE AN INCREASE DURING COVID-19
- ○ 25% ARE CONCERNED THAT BAD ACTORS WILL TARGET PEOPLE WORKING FROM HOME
- ○ FOLLOWING COVID-19, NEARLY A THIRD INTEND TO KEEP LEARNINGS OF INCREASING IT SECURITY TRAINING AND 24/7 IT SUPPORT

Bitdefender

A LACK OF FORWARD PLANNING COMES AT GREAT RISK

Half of infosec professionals (50%) revealed that their organisations didn't have a contingency plan in place, or didn't know if they did, for a situation like COVID-19 or a similar scenario.



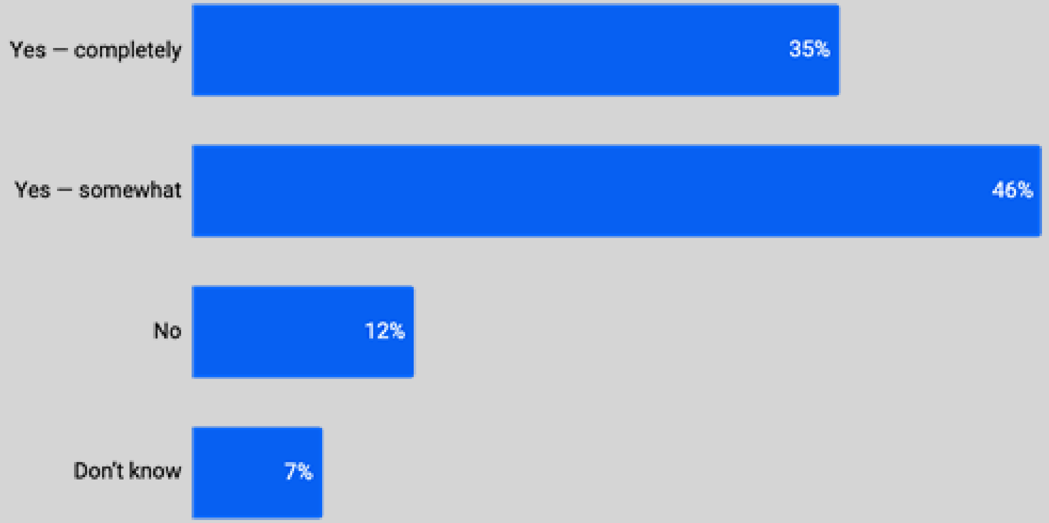
Question: Did your organisation have a contingency plan in place for a situation like COVID-19 or something similar that could have resulted in a similar outcome (eg. people working from home)?

Bitdefender

86% of infosec professionals admitted that attacks in the most common attack vectors were on the rise during COVID-19.

BUSINESS OPERATIONS WILL CHANGE LONG-TERM

Infosec professionals know that strategic changes need to be made rapidly. The significant majority (81%) believe that COVID-19 will change the way their businesses operate in the long-term — a figure that jumps to 92% for those working in energy and 87% for those working in hospitality.



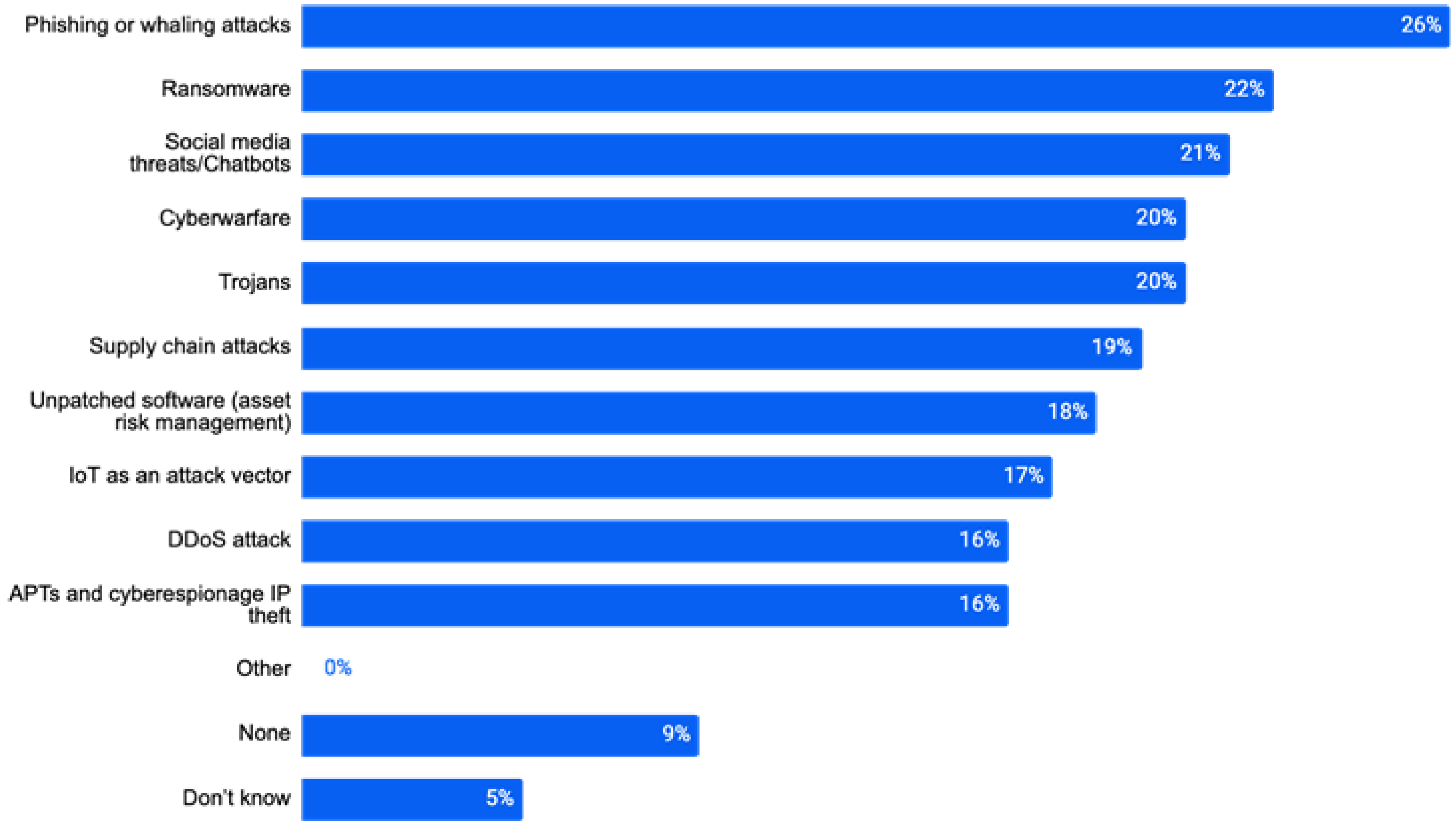
Question: Do you believe the COVID-19 pandemic will change the way your business operates long-term?

THE RISKS ARE IMMEDIATE

and felt by some more than others

THERE'S AN UNDENIABLE BELIEF THAT ATTACKS ARE ON THE RISE DURING COVID-19

Rapid changes to business however often pose excellent opportunities for malicious actors to gain access to corporate information. Infosec professionals report that, in their opinion, phishing or whaling attacks (26%), ransomware (22%), social media threats/chatbots (21%), cyberwarfare (20%), trojans (20%) and supply chain attacks (19%), have risen during the pandemic — and that is to name but a few attack vectors.

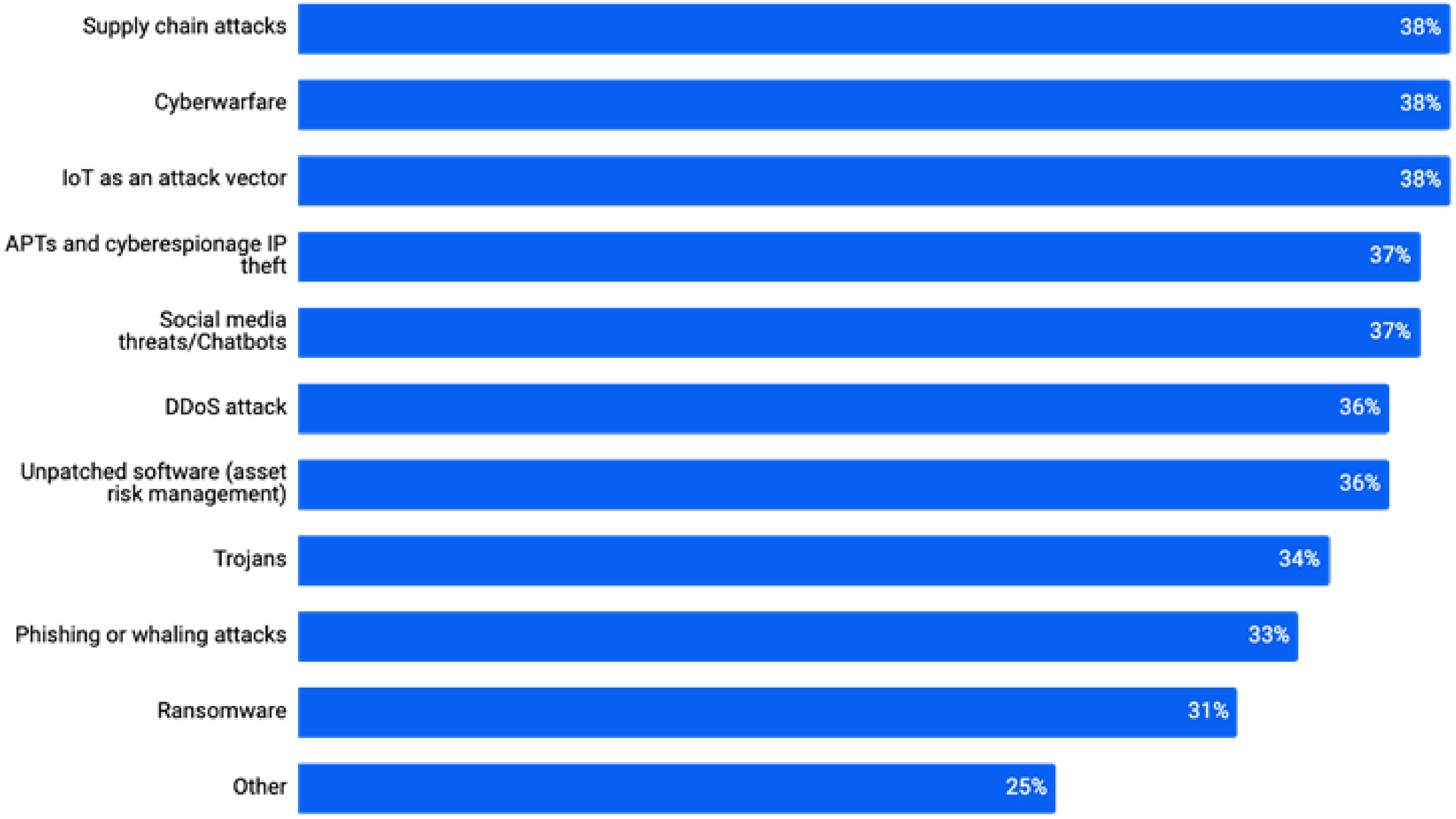


Question: In your opinion, which of the following attacks, if any, increased within your company during COVID-19?

Bitdefender

SUPPLY CHAIN ATTACKS, CYBERWARFARE AND IoT AS AN ATTACK VECTOR ARE THE BIGGEST CONCERNS

While this perceived rise in attacks is alarming, the rate at which attacks have seemingly increased is even more concerning. According to infosec professionals, they believe supply chain attacks, cyberwarfare and IoT as an attack vector were up by 38%. In addition, ransomware was believed to be up by 31%, and DDoS attacks by 36%.

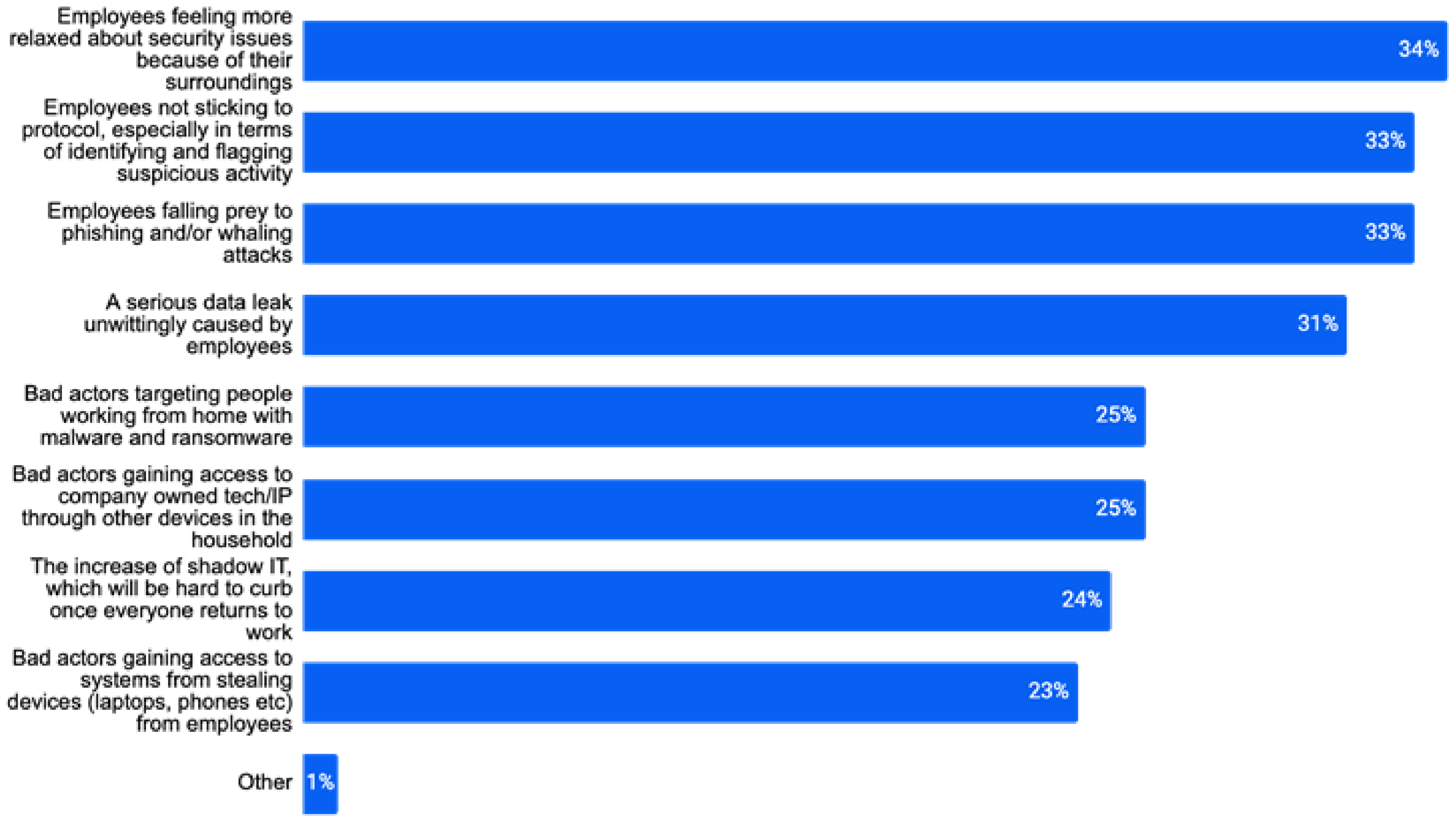


Question: How much did you see these attacks increase by?

Bitdefender

EMPLOYEES WORKING FROM HOME NOW, AND IN THE FUTURE, RAISE MORE CONCERNS FOR INFOSEC PROFESSIONALS

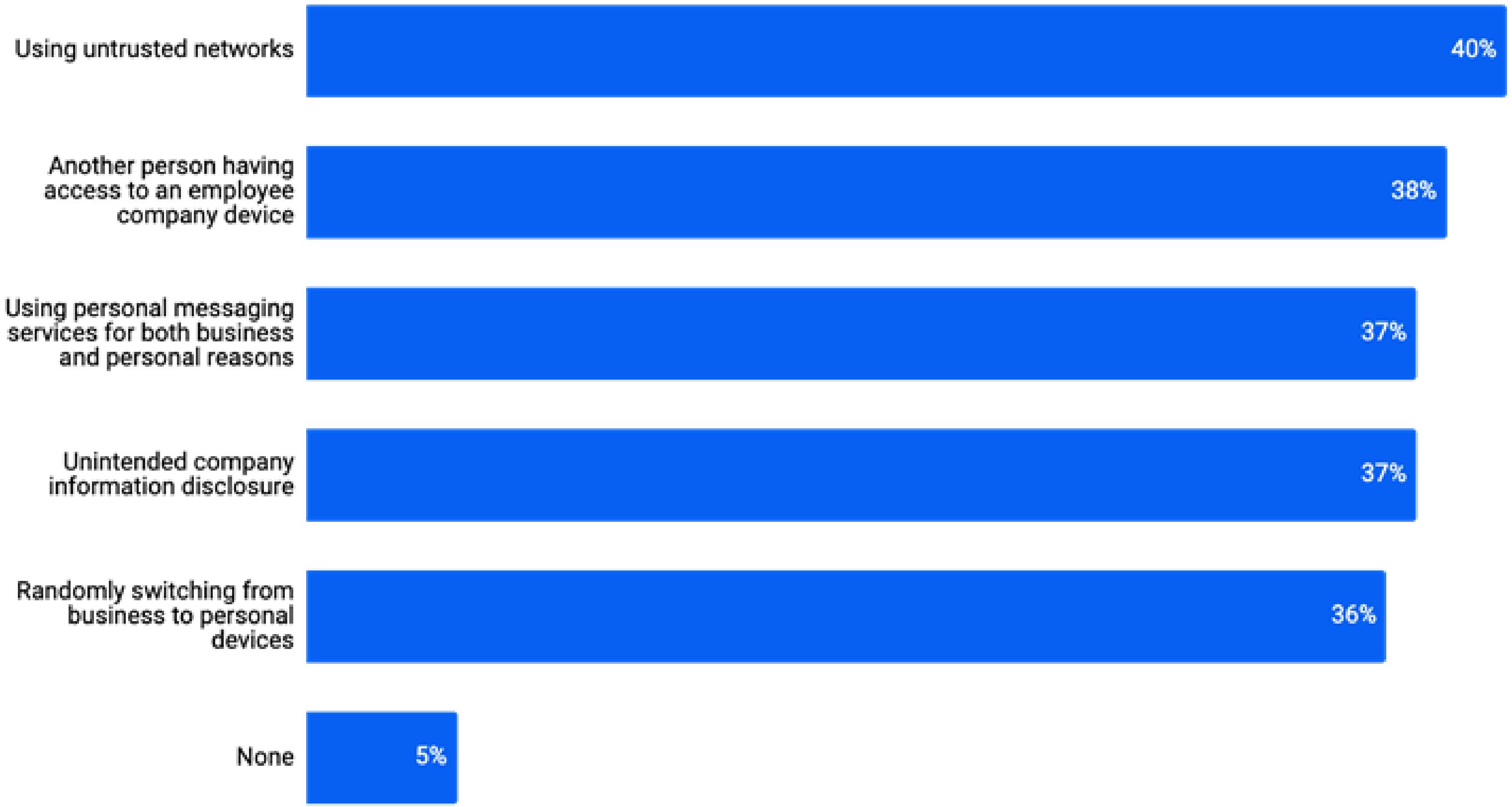
As more employees work from home than ever during the pandemic and possibly many more will want to in the future, infosec professionals are concerned about the security implications. More than one in three (34%) say they fear that employees are feeling more relaxed about security issues because of their surroundings, while others say that employees not sticking to protocol, especially in terms of identifying and flagging suspicious activity, is a worry (33%).



Question: What security risks are you most concerned about when employees work from home? (Not just in the context of COVID-19 but in general)

OUTSIDE OF ATTACK VECTORS, THERE ARE OTHER RISK FACTORS IN EMPLOYEES WORKING FROM HOME

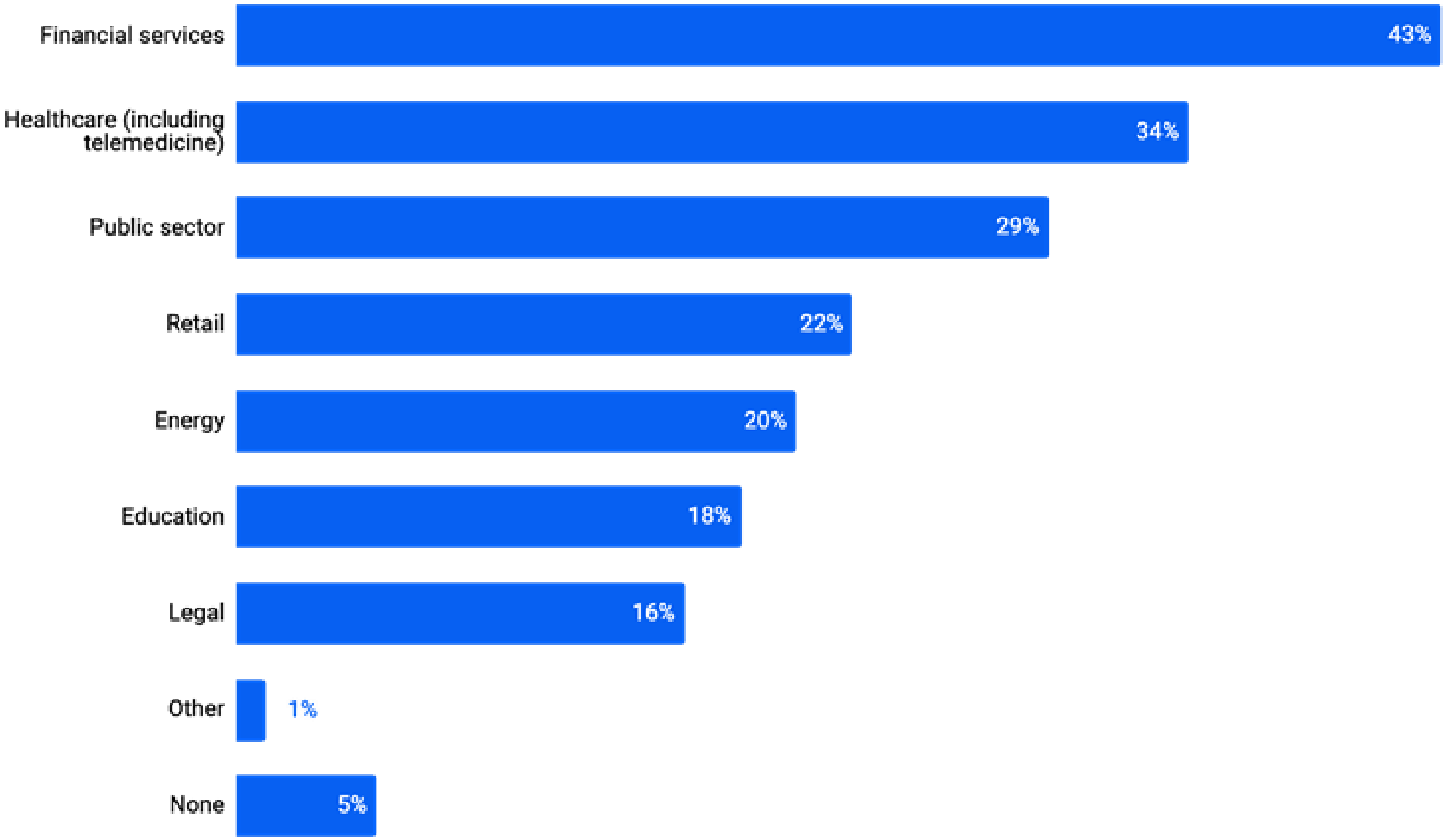
Infosec professionals have also identified specific risks related to home working. Two in five say that employees using untrusted networks is a risk to their organisation, and 38% say there is a definitive risk in another person having access to an employee company device. But the risk factors don't end there. Just over a third (37%) go on to say that using personal messaging services for both business and personal reasons poses a risk, and they also see unintended company information disclosure as a hazard to contend with.



Question: What are the security risks for your organisation when employees are working remotely?

FINANCIAL SERVICES AND HEALTHCARE ARE BELIEVED TO BE THE HARDEST HIT INDUSTRIES

While there is no doubt that all industries are at risk of cybercrime, respondents revealed that they believe that financial services (43%), healthcare (including telemedicine) 34%, and the public sector (29%) to be the hardest hit industries in terms of increase in cyber security attacks during COVID-19.



Question: Which of the following sectors, if any, do you believe would have seen the biggest increase in cyber attacks during COVID-19?

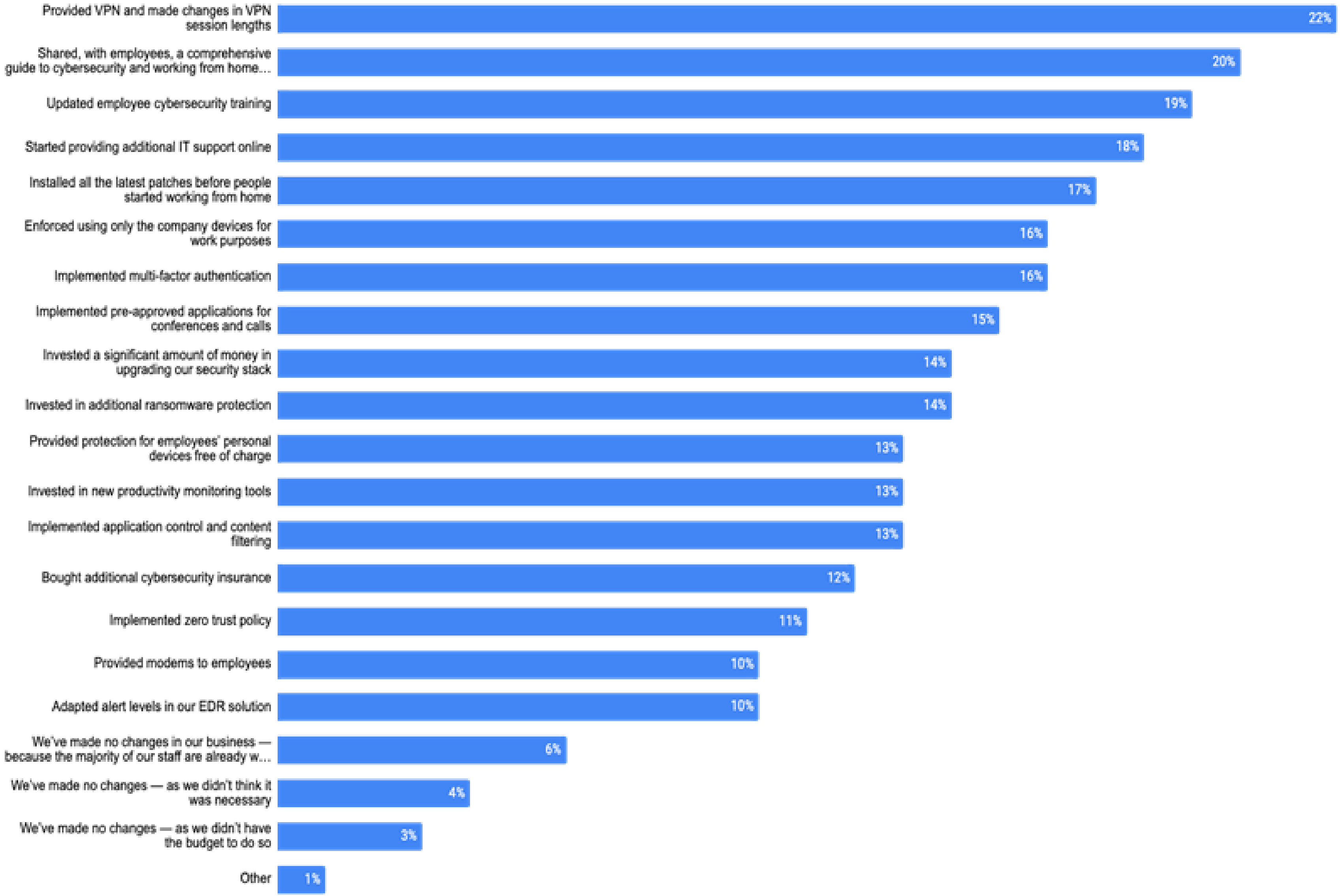
Bitdefender

CHANGE IS AFOOT

and long-term plans are unfolding

MULTIPLE CHANGES ARE ALREADY TAKING PLACE IN SECURITY STRATEGY, YET INVESTMENT IN KEY AREAS REMAINS LOW

As a result of the increase in home working, many changes have been made to security strategies. Yet, despite their fears of a rise in attacks, only 14% have invested a significant amount of money in upgrading security stacks, 12% have bought additional cybersecurity insurance, and only 11% have implemented a zero trust policy — all of which indicates more changes are still to be made.

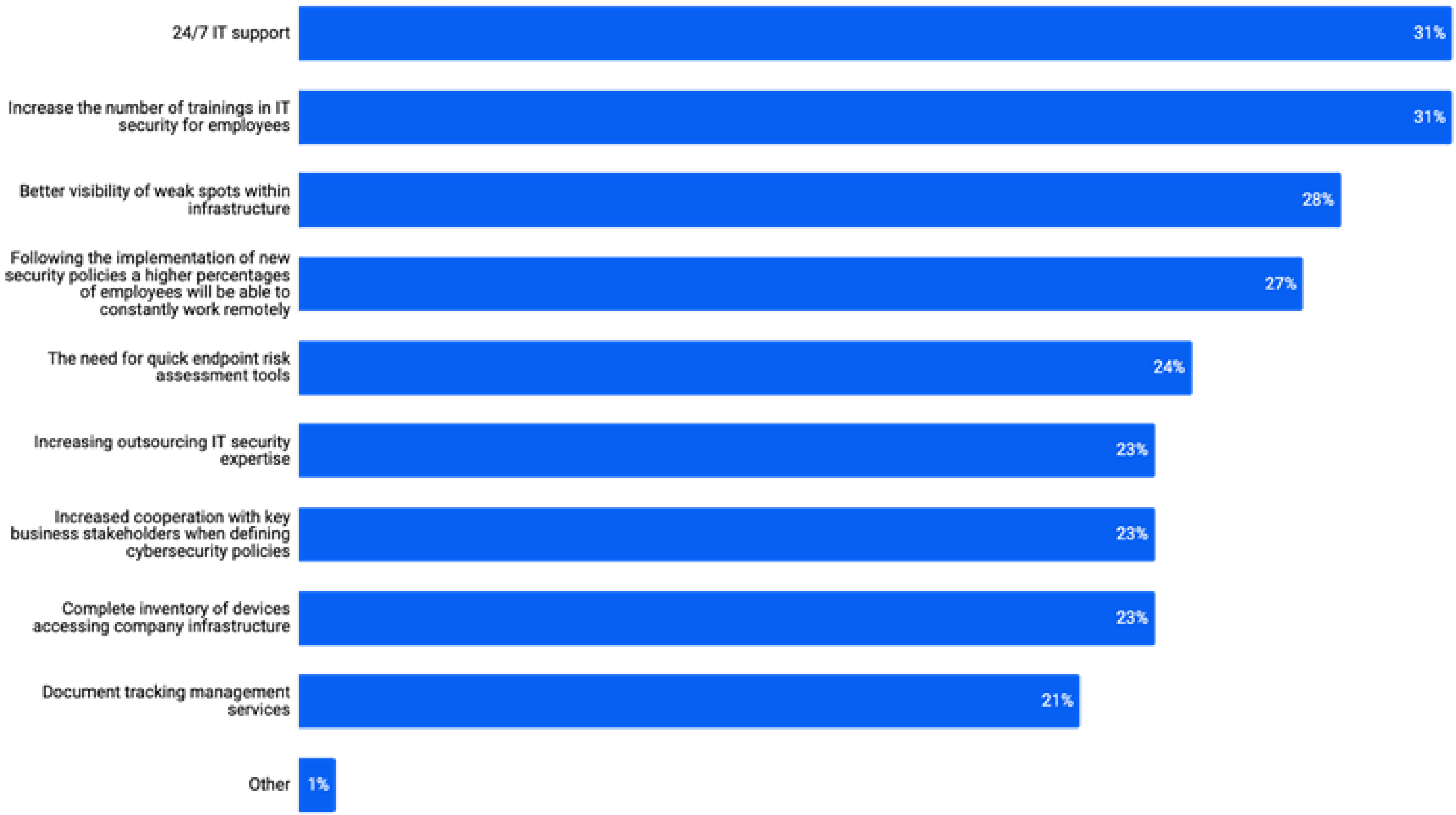


Question: Have you made any changes to your security strategy as a result of more people working from home?' what changes have you made?

Bitdefender

COVID-19 HAS PROVIDED AN OPPORTUNITY TO REASSESS STRATEGY, AND KEY LEARNINGS WILL BE TAKEN FORWARD

The pandemic has provided a valuable opportunity to infosec professionals to learn how to tackle changes in workforce patterns, and how to plan for unexpected events. One in three infosec professionals (31%) say they intend to keep 24/7 IT support, and will increase the number of training sessions in IT security for employees. Almost a quarter (23%) have also cited that they are going to increase the cooperation with key business stakeholders when defining cybersecurity policies, and an equal percentage will increase outsourcing IT security expertise.



Question: What are the learnings that you intend to keep in your cybersecurity policy long term following COVID-19?

“Change is an undeniable threat to cybersecurity, as is being unprepared. The stakes are high in terms of loss of customer loyalty and trust — not to mention to the bottom line.

“COVID-19 has however presented infosec professionals with the opportunity to reassess their infrastructure and refocus on what end users/employees really need and want, in terms of cybersecurity support. The 10 in 10 Indelible Impact of COVID-19 on Cybersecurity Study, reveals that unprecedented change does pose risks, but that it also provides an opportunity to reassess strategy. It is also evident that, despite identifying risks, there is still a need for further investigation into what investments need to be made to ensure that corporate data and employees are both safe from bad actors. While it’s a challenge to make changes now, it will shore up business for the future and many more unknown scenarios.”

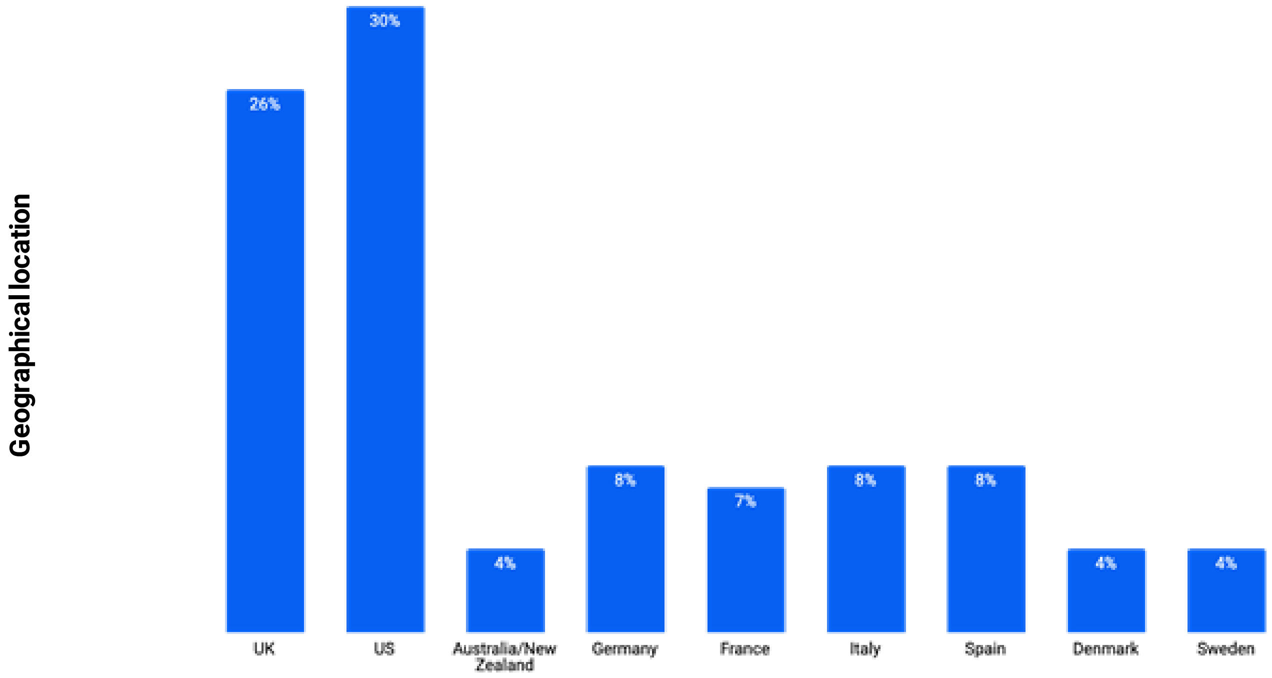
Liviu Arsene, Global Cybersecurity Researcher at Bitdefender.

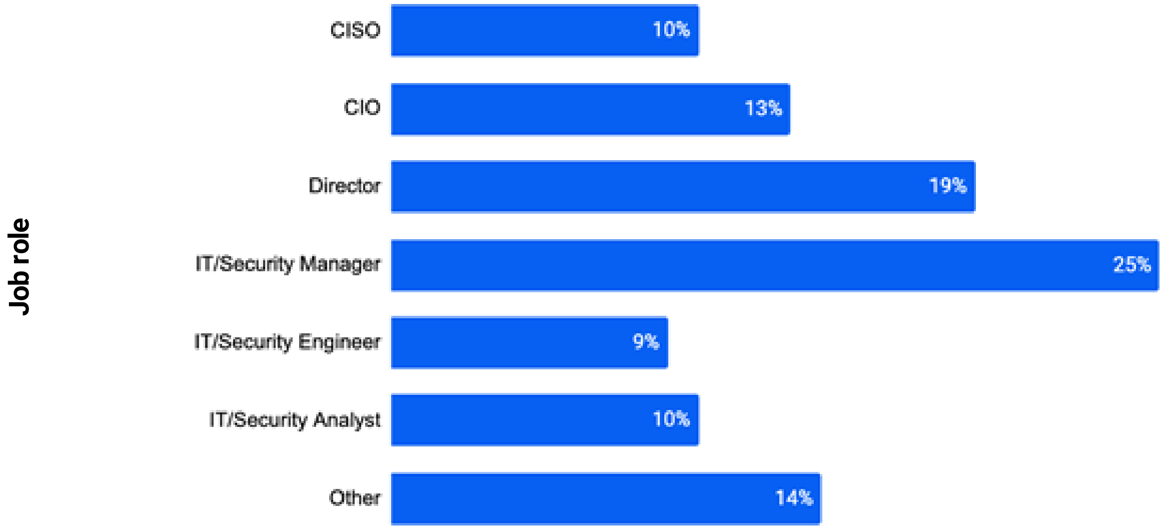
ABOUT THE RESEARCH

The Indelible Impact of COVID-19 on Cybersecurity Study was conducted among 6,724 Security and IT workers in May 2020 across the UK, US, Australia/New Zealand, Germany, France, Italy, Spain, Denmark and Sweden. Representing a broad cross-section of organisations and industries, from fledgeling SMEs, through to publicly listed 10,000+ person enterprises. The report, which will form part of the yet to be released 10 in 10 Study, details the pressures faced by IT professionals during the COVID-19, how these pressures are testing the effectiveness of security measures and the changes they will need to make within their organisations as a result.

All audience members utilise and/or have decision-making power over data security solutions and software security products. The interviews were conducted online by Sapio Research in May 2019 using an email invitation and an online survey.

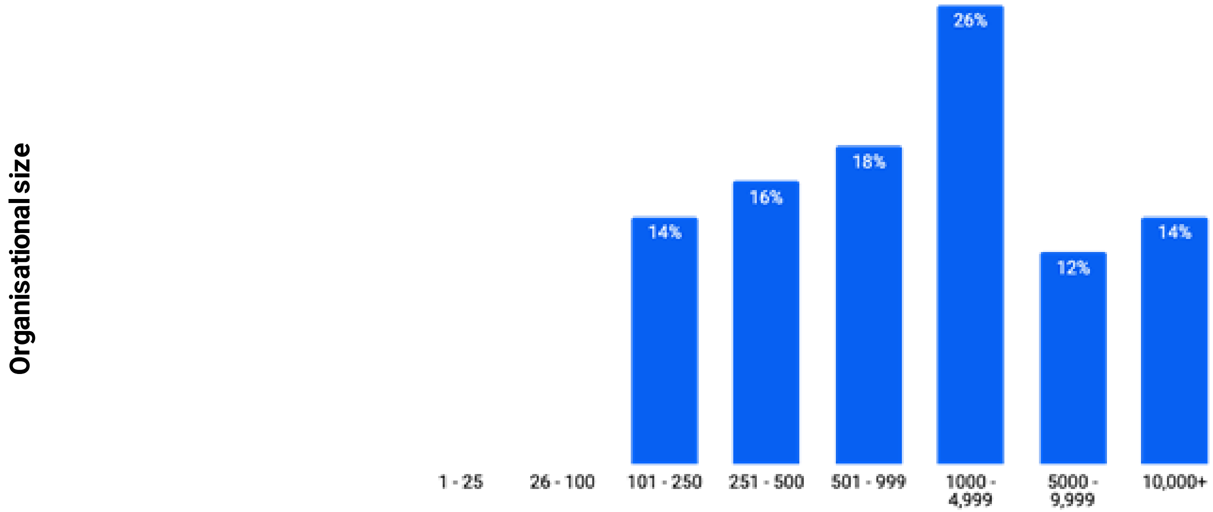
RESPONDENTS BY GEOGRAPHY AND JOB ROLE

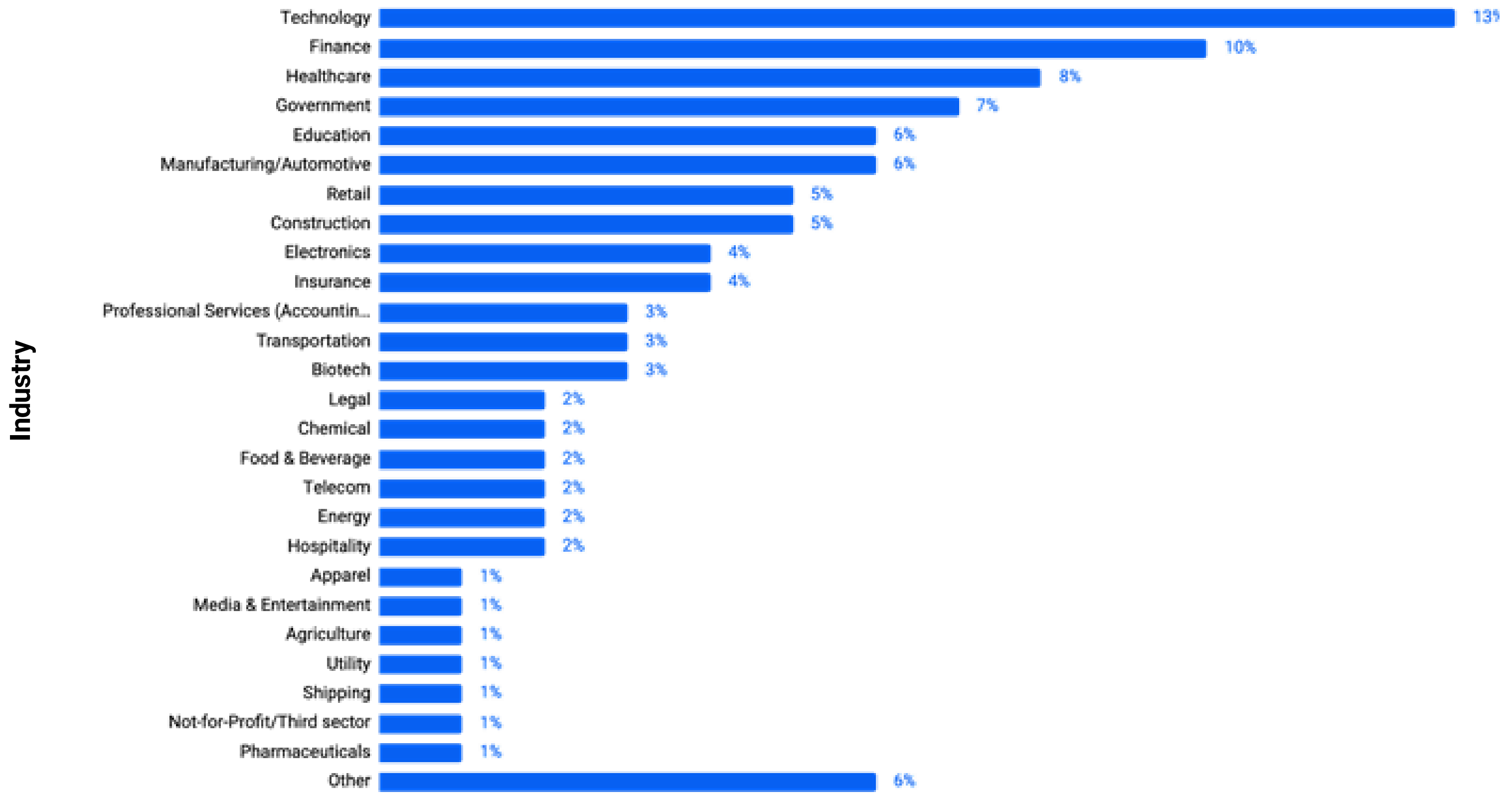




Bitdefender

RESPONDENTS BY ORGANISATIONAL SIZE AND INDUSTRY





Bitdefender

ABOUT BITDEFENDER

Contact Us

Bitdefender is a global cybersecurity leader protecting over 500 million systems in more than 150 countries. Since 2001, Bitdefender innovation has consistently delivered award-winning security products and threat intelligence for the smart connected home, mobile users, modern businesses and their networks, devices, data centers and Cloud infrastructure.

Today, Bitdefender and its Labs is also the provider vendor of choice, embedded in over 38% of the world's security solutions. Recognized by industry, respected by vendors and evangelized by customers, Bitdefender is the cybersecurity company you can trust and rely on.

Contact Us

bitdefender.com

publicrelations@bitdefender.com

twitter.com/Bitdefender_Ent

Bitdefender

Bitdefender®

WWW.BITDEFENDER.COM