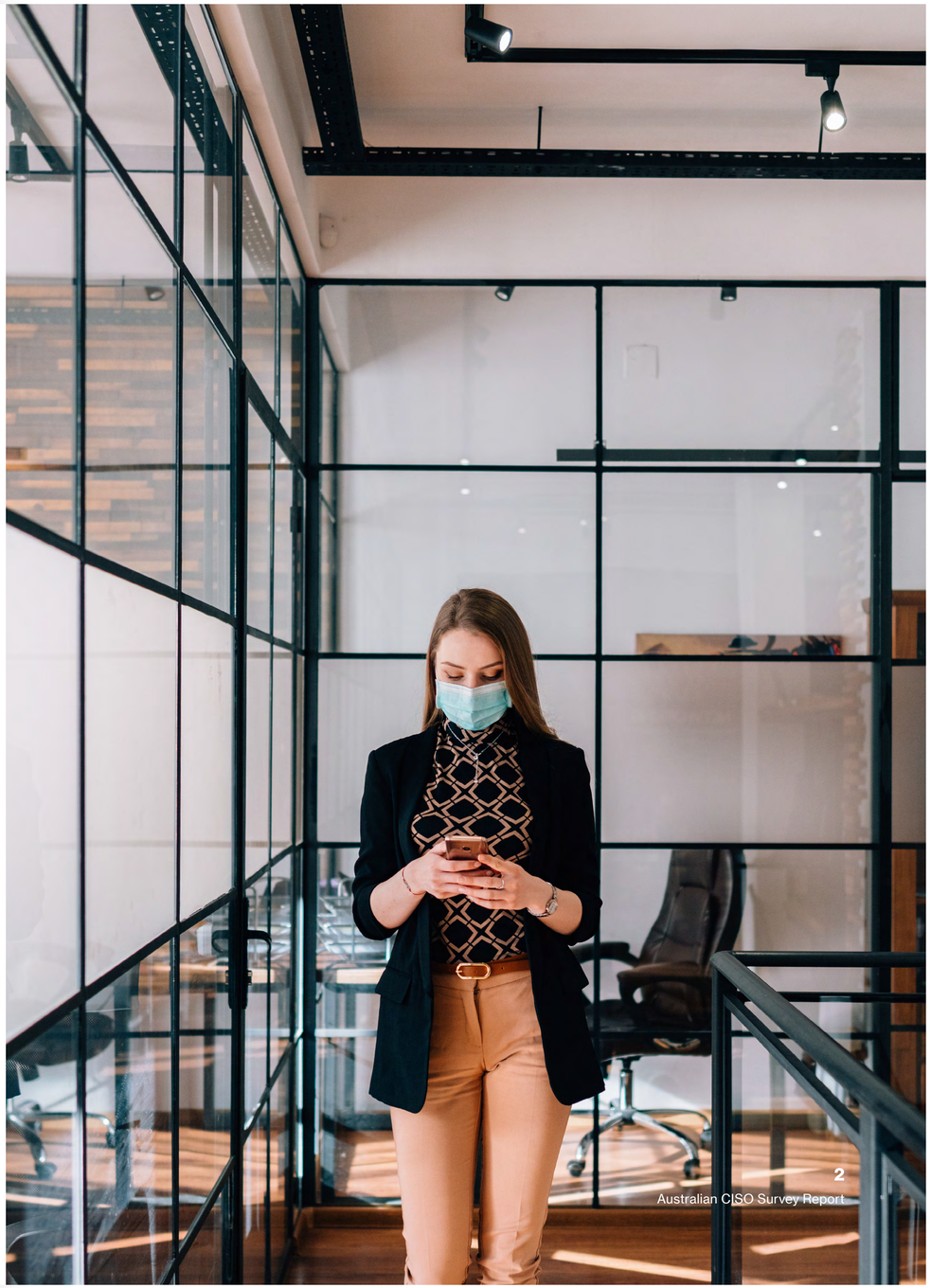
Ivanti's Australian CISO Survey: How the Pandemic Has Shifted CISO Priorities

Introduction

The COVID-19 pandemic has forced organisations to shift to an Everywhere Workplace model of working. Today, IT infrastructures are everywhere, and distributed employees need access to corporate data wherever they work, on any device. As organisations around the world consider making remote work a permanent option for their employees moving forward, we wanted to understand how the pandemic and mass shift to remote work has impacted CISOs. How has the changing IT security landscape challenged them and changed their priorities?

We commissioned independent market research agency Vanson Bourne to conduct a study examining how CISOs across Australia have responded to the COVID-19 crisis and the new remote work environment. Between March and April 2021, 80 CISOs from large enterprise organisations in Australia were interviewed to better understand their evolving security strategies.

The survey revealed that the shift to the Everywhere Workplace has forced CISOs to ensure that working from home is just as secure as working from the office. As a result, CISOs are now more focused on mitigating mobile security risks than combating enterprise network threats.



The Security Landscape Has Changed

The Everywhere Workplace has changed the cybersecurity battleground for the foreseeable future. Almost nine in ten (88%) of survey respondents agreed that remote work has accelerated the demise of the traditional network perimeter, which CISOs had been accustomed to defending. Mobile devices are now everywhere and have access to practically everything, which creates new security challenges for IT departments. At the same time, cybersecurity threats targeted at remote workers are reaching catastrophic new heights.

The majority (90%) of CISOs agreed that mobile devices have now become the focal point of their cybersecurity strategies, and two thirds (66%) stated that passwords are no longer an effective means of protecting enterprise data, as hackers are increasingly targeting remote workers and mobile devices.

When pressed on the main IT security challenges that their organisations have faced during the pandemic, CISOs overwhelmingly agreed that they have struggled to ensure that only trusted users, devices, networks, and apps can access company data.

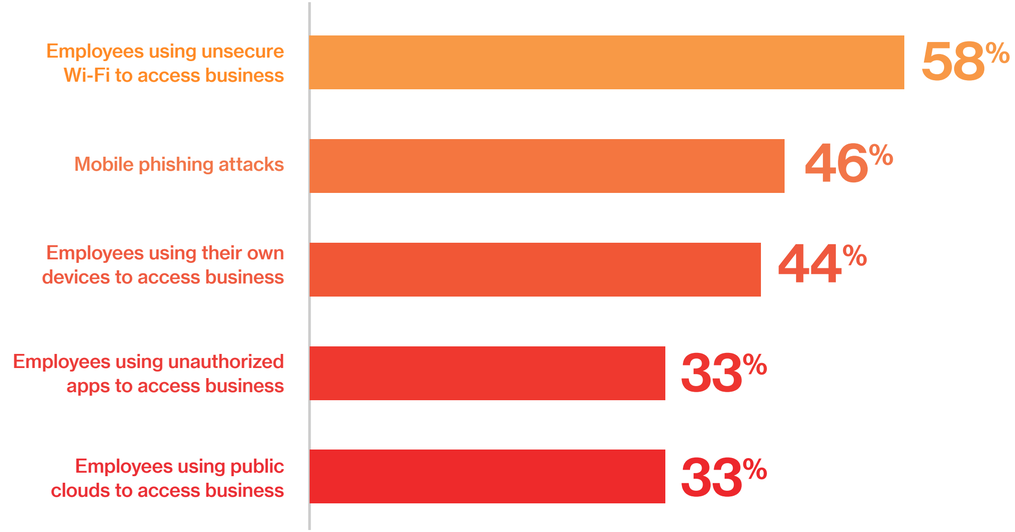
90%

of CISOs claim that mobile devices have now become the focal point of their cybersecurity strategies.

Top IT Security Challenges Facing CISOs During the Pandemic

Over half (58%) of respondents cited employees leveraging unsecure Wi-Fi to access business resources as a main IT security challenge. Almost half (46%) cited mobile phishing attacks and over two-fifths (44%) cited employees using their own devices to access corporate data as other top IT security challenges during the pandemic.

Unfortunately, hackers are taking advantage of security gaps in the Everywhere Workplace by increasingly targeting mobile devices and applications with sophisticated phishing attacks. And these mobile phishing attacks are likely to succeed, as it is very hard to verify the authenticity of links on a mobile device. The mobile user interface also makes it difficult to access and view key information, while prompting users to make fast decisions.



Zero Trust

The explosion of endpoints, devices, and data required for remote work has been matched by an increase in cybersecurity threats. Securing this rapidly expanding threat landscape is a major headache for CISOs, who need to protect mobile employees without limiting access to the corporate data they need when they need it.

By implementing a zero trust security strategy that seeks to verify every user, device, app, and network before granting access to business resources, CISOs ensure employees stay productive and secure, wherever they work.

CISO Priorities are Evolving

The Everywhere Workplace is undoubtedly here to stay; in fact, a recent Gartner Survey found that 80% of company leaders around the world plan to let employees work remotely from now on, at least part of the time.

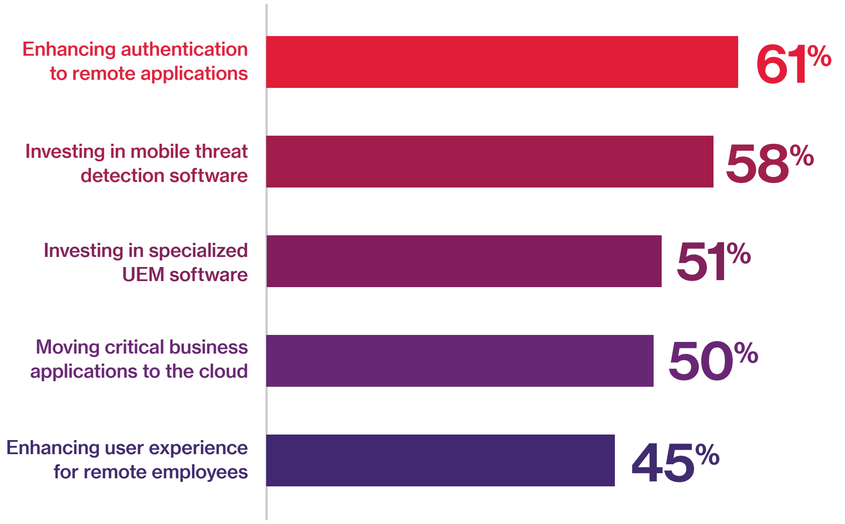
As a result, CISOs are placing greater emphasis on enabling, securing, and optimizing mobile work environments. While 91% of CISOs stated that their organisations had effective solutions in place to enable employees to work remotely at the start of the pandemic, almost all of them (94%) also agreed that they would benefit from deploying further IT security measures to enable remote working in the year ahead.

When pressed on what these measures would specifically include, the CISOs gave a range of responses that included tightening mobile security and improving the remote work experience for employees. To support these initiatives, almost two-thirds (61%) said improving user authentication to remote applications will be a priority in 2021, while a similar number (58%) said they will likely invest in mobile threat detection software in the coming year.

Meanwhile, more than half (51%) said investing in specialised endpoint management software will be a top priority. Half of the respondents said moving critical business applications to the cloud will be essential, and 45% said enhancing user experience for remote employees will be a main objective for the year ahead.

94%

of CISOs agree they would benefit from deploying further IT security measures to enable remote working in the year ahead



Remote Work is Increasing IT Security Budgets

The study also sought to understand how CISOs plan to adjust and reallocate their IT security budgets to address the new threat landscape. The study found that on average in 2020, CISOs across Australia had a total IT security budget of $6,128,171, with a large portion (49%) being spent on specialised UEM software to manage and secure endpoints and mitigate mobile security threats.

However, IT security budgets are expected to grow in 2021 to support the additional IT security measures needed to protect remote workforces. More than four in five (83%) of CISOs said their overall IT security budget is likely to increase in 2021, with 19% claiming it will greatly increase.

Considering the growing number of endpoints and devices across the Everywhere Workplace, 86% of CISOs said that their investments in specialized UEM software will increase during 2021. To overcome the pain of passwords, almost four in five (79%) CISOs said they also plan to increase their investment in biometric authentication technologies.

By increasing their investment in these two areas, CISOs will be able to better discover, manage and secure the devices, applications, and networks that employees need to work from home, while also delivering a seamless end user experience for employees.

86%

of CISOs will increase their investment in specialized UEM software in 2021

Conclusion

These survey results illustrate the dramatic shift in priorities for CISOs in 2020. Remote work has accelerated the death of the traditional network perimeter and has put mobile security firmly in the spotlight. The explosion of mobile devices, apps, and users – combined with the exponential growth in cybersecurity threats – means that CISOs must now place greater emphasis on enabling, securing, and optimizing mobile work environments.

To this end, every CISO should urgently adopt a zero trust security strategy to ensure that only trusted users can access corporate data. In addition, IT should invest in automation technologies that can discover, manage, secure and service all endpoints, devices and data. Not only then will these new approaches help CISOs support a more secure remote infrastructure, they will also help IT reduce time-consuming management tasks and allocate resources to more strategic initiatives.

Methodology

Ivanti commissioned independent technology market research specialist Vanson Bourne to undertake the quantitative research upon which this report is based. A total of 80 CISOs were interviewed in Australia between March and April 2021. Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were allowed to participate.

Copyright © 2021, Ivanti. All rights reserved. IVI-2588 06/21 SR/FG

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT applications and data over various networks to stay productive as they work from anywhere. The Ivanti Neurons automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a unified IT platform that enables devices to self-heal and self-secure and empowers users to self-service. Over 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure, and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com and follow @GoIvanti.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com

ivanti.com
1.800.982.2130
sales@ivanti.com