ONAPSIS TURNKEY

SAP Security Survey Report 2021

A Turnkey report, in conjunction with Onapsis

www.turnkeyconsulting.com

Contents

SAP Security Report

01 Introduction

Turnkey and Onapsis have joined forces to explore customer views on the vulnerability of SAP systems to external threats.

Our online survey was conducted with more than 100 SAP customers from the United Kingdom, Europe, Asia and the United States. All respondents hold significant influence (managerial level or above) within a cyber security related function, in organisations representing over 15 different industries.

A range of questions looked at customers' current preparedness to deal external attack. But specifically, we wanted to explore the perception that SAP is protected because it is within the internal network - and how this affects customers' levels of defence.

We hope the findings within this report can help inform businesses on their SAP security journey, and help them make the right decisions to keep their data and applications safe. We wish to thank all who took part in this research, and thank you for taking an interest in the report.

"

This report is supported by commentary from Turnkey's Application and Cyber Security Practice Director, Tom Venables. Tom has almost 20 years' experience in helping large, enterprise-level organisations protect their business-critical SAP applications.

E: info@turnkeyconsulting.com

02

Executive summary

Executive summary

Among the many findings that our survey has uncovered, one key trend is that SAP security is seen as a challenge by administrators, but that it isn't necessarily linked to the wider management and understanding of IT risk.

Much of this is down to administrators that know how to secure access to applications, but don't have the ABAP or BASIS background to understand needs around code scanning and patch management. These areas, along with secure system configuration and privilege misuse, are considered lower priority by many organisations, given the lower numbers of respondents that are at high levels of maturity in managing them.

Respondents to the survey recognise that the SAP landscape is evolving, with only 27% not considering a move to S/4 HANA or remaining undecided at this stage. But despite this, there is a lack of realisation that external attacks are of serious concern, even though digital transformation, cloud-first approaches and mobile access are opening SAP systems up to greater levels of external threat.

There are many ways in which this gap in understanding can be addressed. One is education: when SAP administrators and users alike are well trained in cyber security awareness, they will know the relevant risks and be less likely to fall foul of common avenues of attack. Another is to take the same 'by design' approach used for the wider IT estate and apply it to SAP, so that the core principles of cyber defence are embraced. And a third is to break down silos between the SAP system and wider IT risk management, and pool resources to protect the overall estate and close off any gaps.

Overall, the results make clear that organisations are making some progress in how they protect their SAP systems, but there is still lots of catching up to do. We hope these findings will help SAP customers understand how they can better protect themselves against an evolving threat landscape.

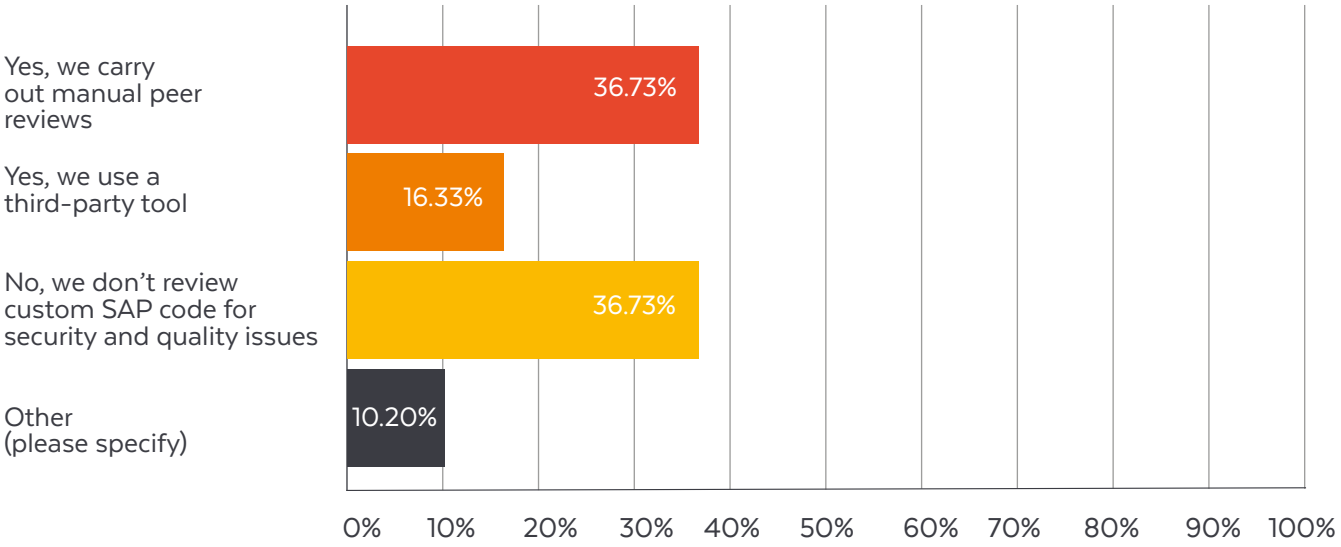
E: info@turnkeyconsulting.com

03 Findings

ONAPSIS TURNKEY

Q1

Do you review custom SAP code for security and quality issues? If so, how?



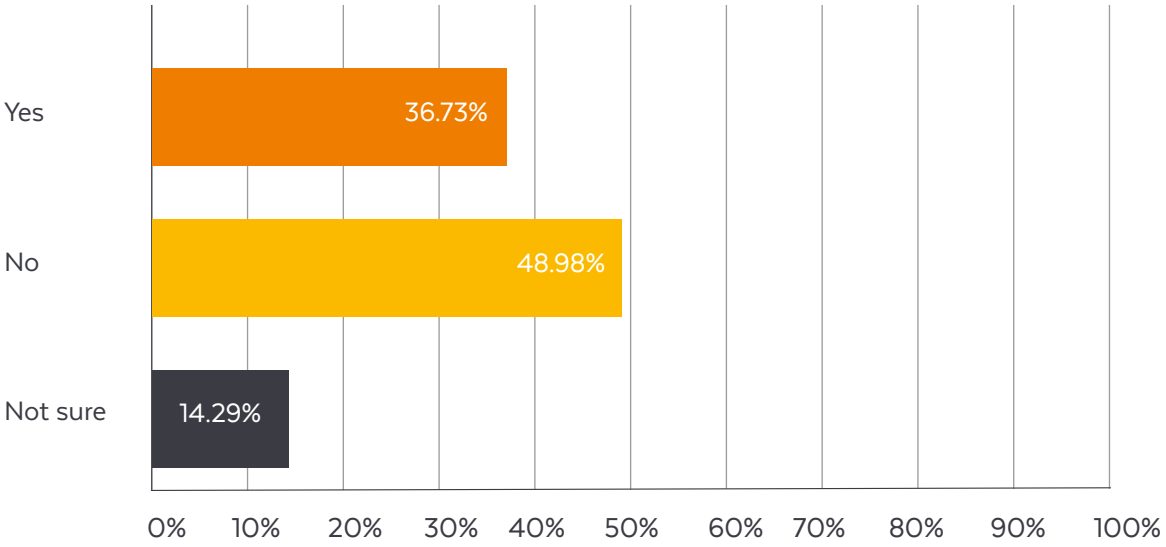
Commentary

Given that the average SAP customer will have approximately 2500 vulnerabilities within their custom code, reviewing this code for security is vitally important. While more than half are conducting these reviews, two-thirds of those who do so are doing them manually, which can be extremely time-consuming and prone to human error. The significant minority that are not reviewing their code are not only leaving themselves more vulnerable to attack, but they are also risking downtime that can be extremely costly to the organisation.

ONAPSIS TURNKEY

Q2

Have you experienced downtime in your SAP landscape as a result of a coding issue?



Commentary

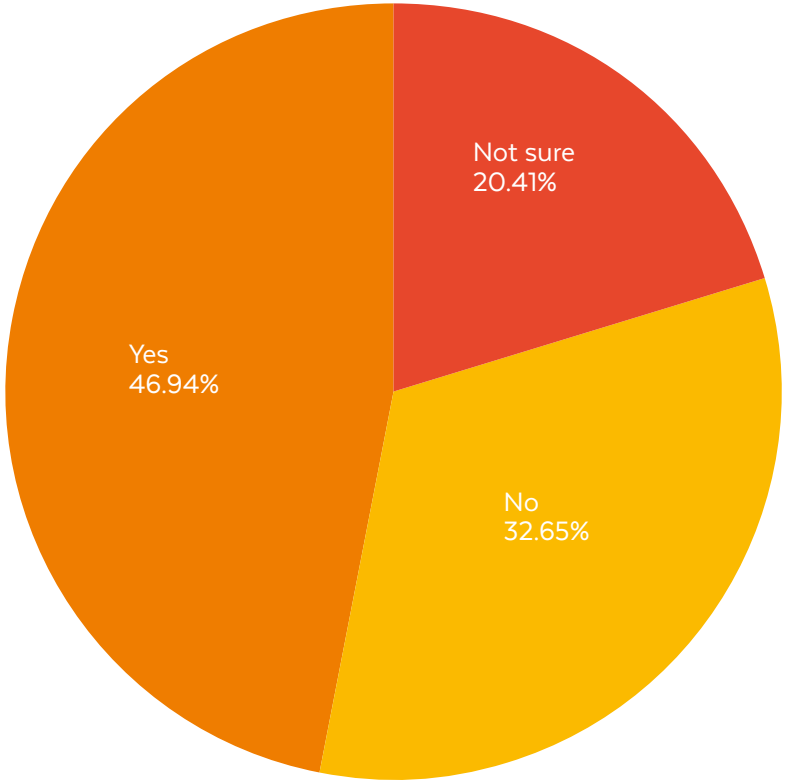
The importance of securing code is highlighted by the fact that more than a third of respondents have experienced SAP downtime because of coding issues. In particular, code injections - where attackers exploit vulnerabilities at code level - are a common source of downtime, financial losses, reputational damage, and non-compliance.

E: info@turnkeyconsulting.com

ONAPSIS TURNKEY

Q3

Do you review code developed by third parties for security and quality issues before importing into your SAP system?



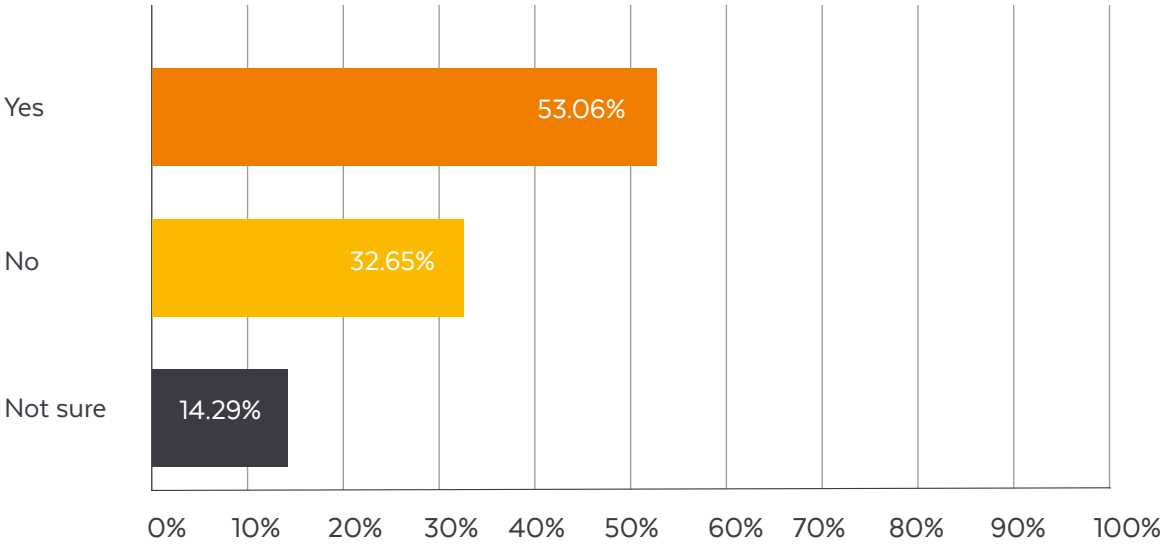
Commentary

Nearly half of respondents ensure third-party code is reviewed before it's imported into their SAP system, which fits in well with a 'zero-trust' approach to security (where it's assumed that a system will be attacked at some point). However, it is concerning that more than half don't review it or aren't sure if the reviews take place. The reasons for this are many: business pressures, lack of resources or because dev teams are distributed and unable to run the reviews effectively, but this doesn't make the impact of a cyber attack any less severe.

ONAPSIS TURNKEY

Q4

Do you have a way to identify insecure or problematic custom code before it hits production systems?



Commentary

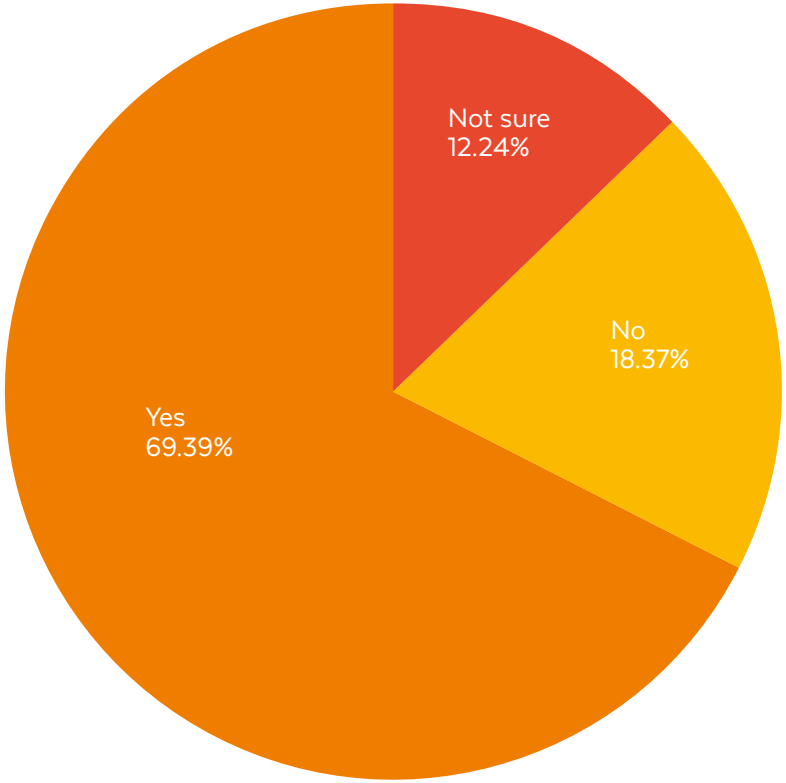
Nearly a third of respondents say they are unable to check over custom code to ensure that anything problematic doesn't reach the SAP system. For many, this will be an issue of capability rather than desire: many organisations don't have the in-house resources to achieve it, and the continued skills shortage within the security sector makes it difficult to obtain the right expertise. However, others are bypassing the checks because of business pressures around getting code up and running quickly. Tools and automation offer the most viable way for organisations to put gating checkpoints in place.

E: info@turnkeyconsulting.com

ONAPSIS TURNKEY

Q5

Can you identify all of the systems and interfaces connected to your SAP landscape?

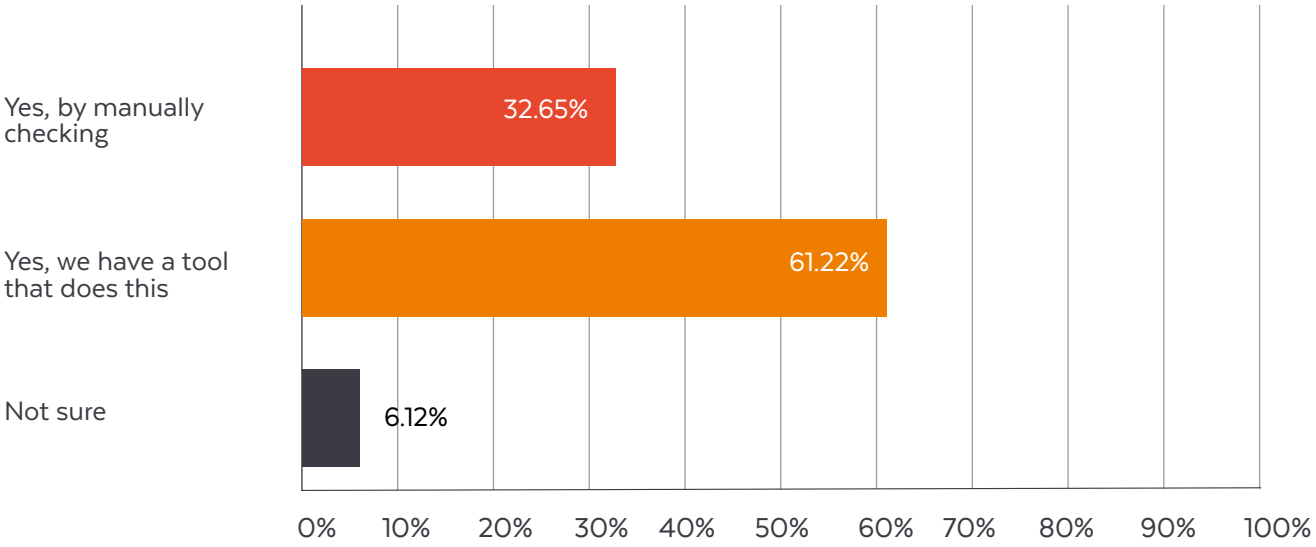


Commentary

The fact that almost 70% of respondents have a full grasp of the SAP topography is encouraging, especially in a climate where business IT estates are becoming more and more complex and interconnected. This complexity may go some way to explaining why so many respondents either can't identify all their connected systems or interfaces, or aren't sure. It should be noted, though, that the identification process may be very time-consuming for many organisations, and this may be a barrier to some organisations in identifying everything.

Q6

Do you have a way to audit user authorizations and roles in SAP?



Commentary

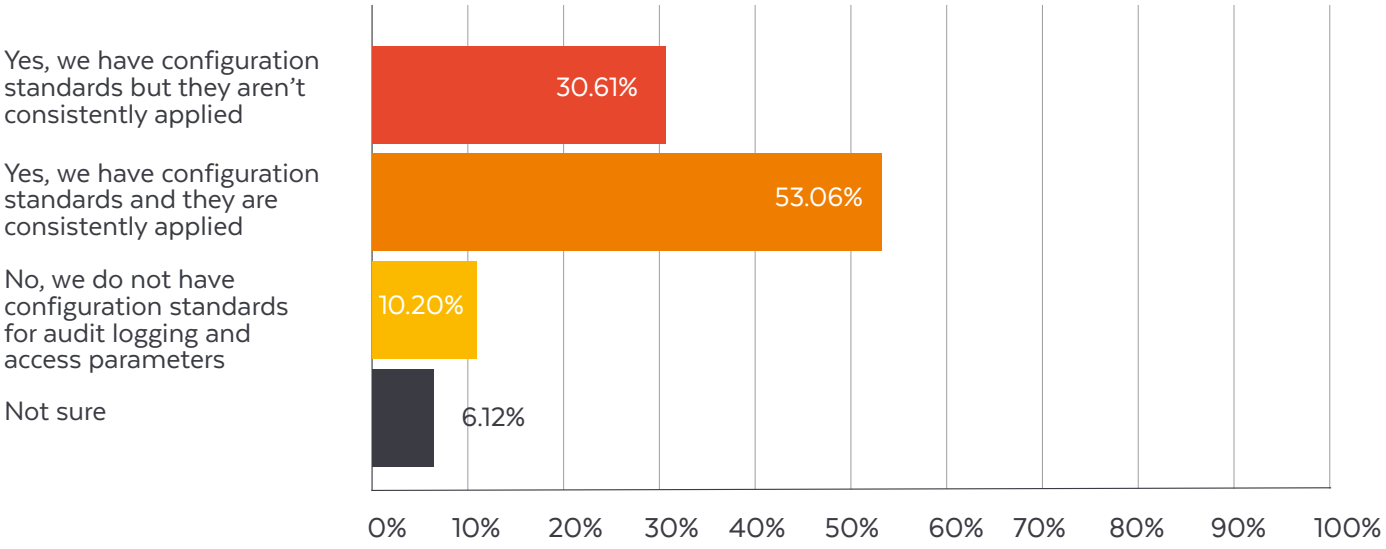
The vast majority of respondents have an audit mechanism in place for user authorisations and roles, but almost a third are still doing so through time-consuming manual checks rather than by using an automated tool. Manual checking becomes even more of a burden in the context of the increasing auditing requirements for SAP systems, including configuration settings, parameter settings, patching and code.

E: info@turnkeyconsulting.com

ONAPSIS TURNKEY

Q7

Do you have standards for configuration of audit logging and access parameters (like password settings) in SAP, and are these consistently applied?



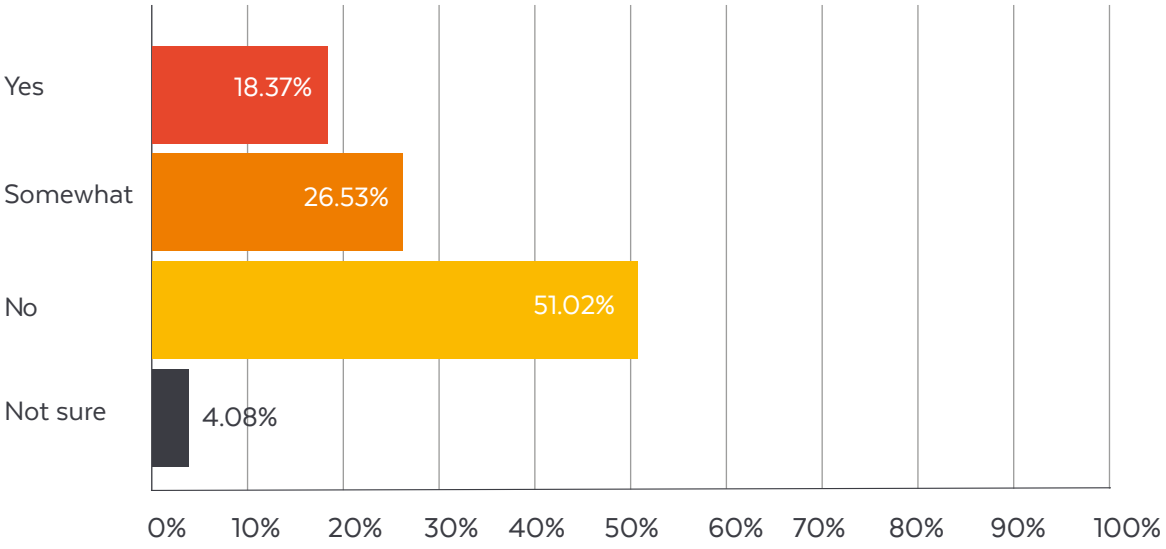
Commentary

It's concerning to find that almost half of respondents either aren't applying configuration standards consistently, or aren't applying them at all. As with other issues in this survey, the amount of time and resources required to apply these standards is considerable: config drift needs checking, and high volumes of log data needs processing. This is therefore another area where automation can assist, along with tools for alerting, monitoring, and change management functions that can keep track of any changes being made.

ONAPSIS TURNKEY

Q8

Would you generally agree with the statement “SAP is within our network, and so is secured against cyber threats”?



Commentary

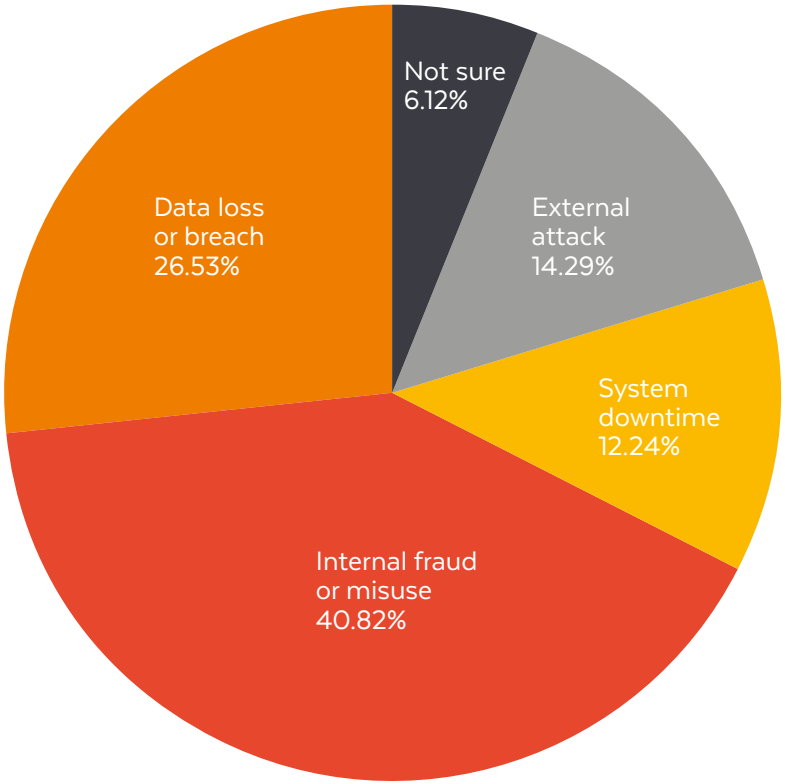
The often misguided perception that SAP is secured against cyber attacks because it sits within an organisation’s internal network is gradually being shattered. A slight majority of respondents disagreed with the view, and less than one in five still felt that it was fully secured by being inside the network. It may well be, however, that those who feel it is fully secured in this situation have the right tools and monitoring in place to cover SAP, or that the level of their internet-facing activity is relatively limited.

E: info@turnkeyconsulting.com

ONAPSIS TURNKEY

Q9

What would you consider is the greatest risk to your SAP systems?



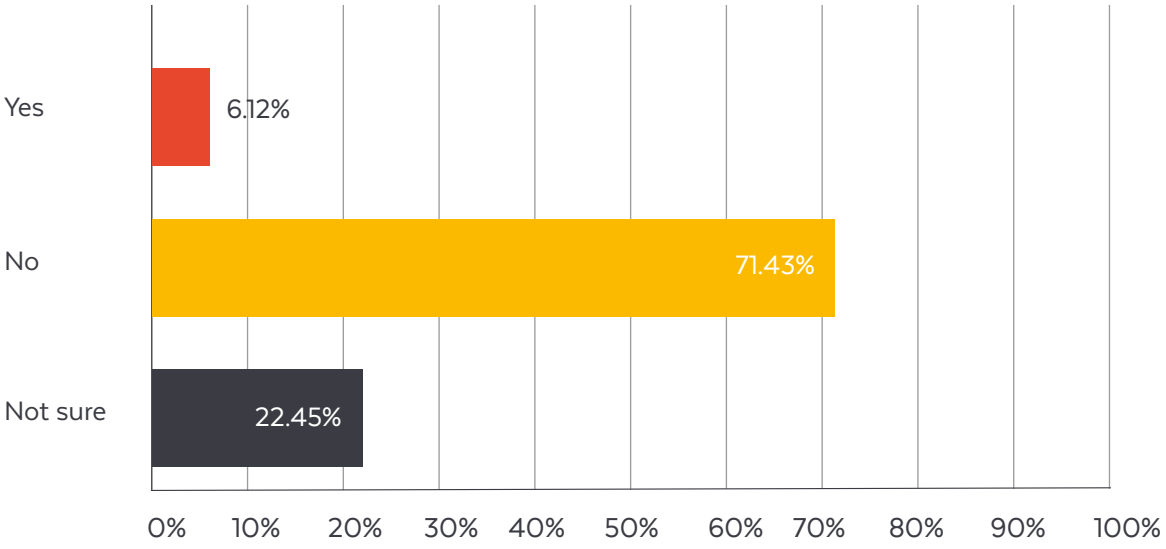
Commentary

External attack is a significant threat to SAP systems - and increasingly so - but only one respondent in seven feels that it's the biggest threat to their systems. More and more malicious actors have realised that SAP often contains highly valuable data and intellectual property; the kind of information that, if lost or inaccessible, would cause major business disruption. Some 40% of respondents still consider their biggest threat to be fraud or misuse from within, but the variety of responses demonstrates that businesses prioritise their focus on where they perceive the biggest risk is.

ONAPSIS TURNKEY

Q10

Has your organization been victim to a data breach related to one or more of your SAP systems in the past two years?



Commentary

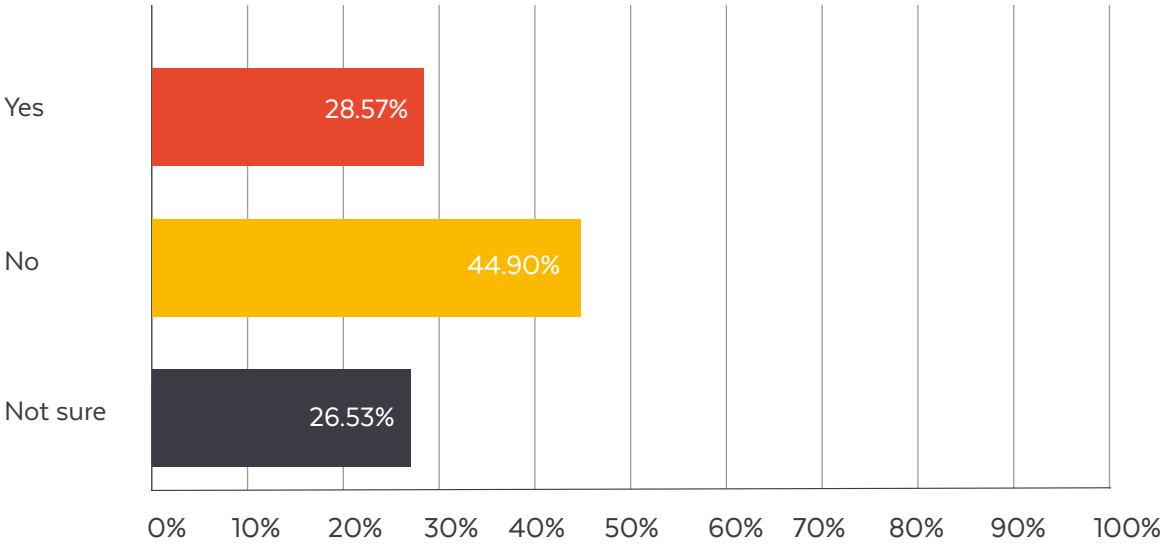
The number of respondents admitting to a recent SAP data breach is lower than expected, but that may be partly down to some firms not wanting to admit to any issues that they've had. It is hoped that those who responded 'no' did so because they have the correct protections in place, but it cannot be ruled out that some of them have simply been fortunate not to have been attacked. The significant proportion of those unsure may have said so because they don't have the ability to monitor their systems and find a breach, or because ownership of this monitoring resides elsewhere within their organisation.

E: info@turnkeyconsulting.com

ONAPSIS TURNKEY

Q11

Do you currently have a vulnerability management program for SAP?



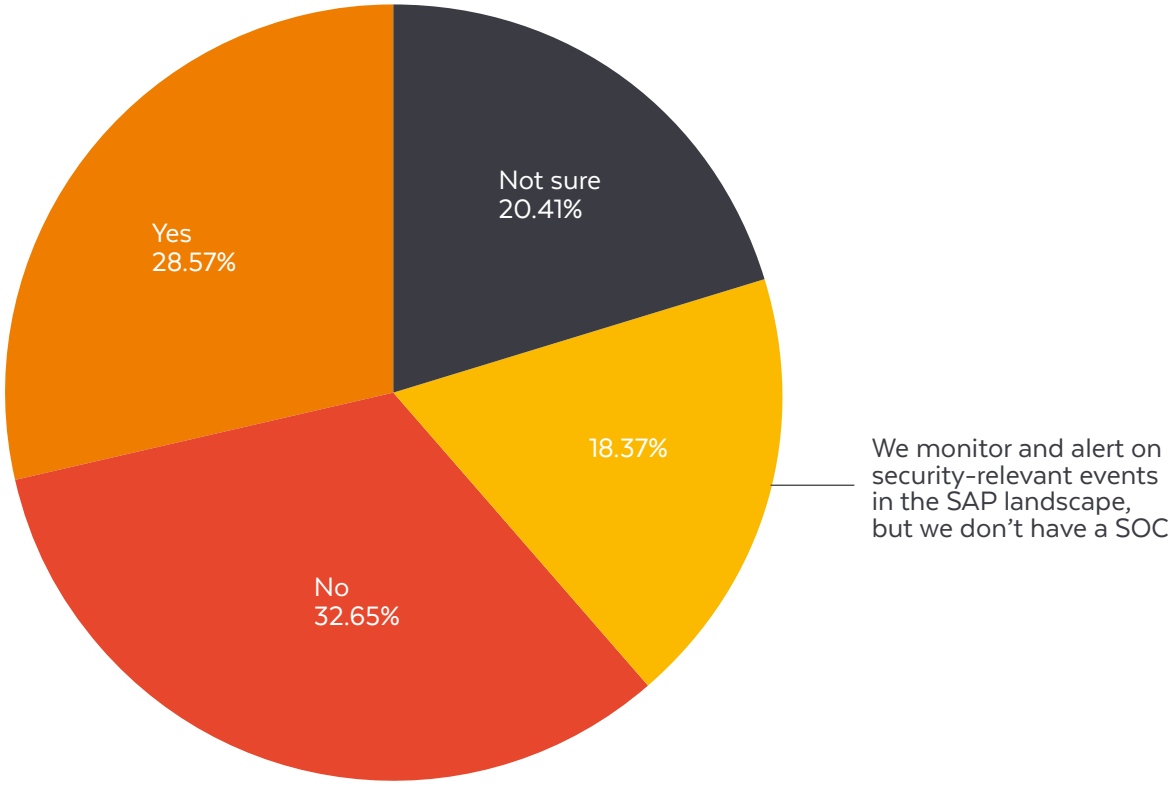
Commentary

Less than 30% of respondents were able to confirm that they have a programme in place to manage the vulnerabilities of their SAP systems. This is concerning at a time when cybercrime has moved far beyond lone hackers to become the domain of organised crime groups. It suggests that SAP application owners haven't kept pace with the demands of cyber security in the same way that a more traditional CISO has had to.

ONAPSIS TURNKEY

Q12

Does your SOC have visibility into SAP security events?



Commentary

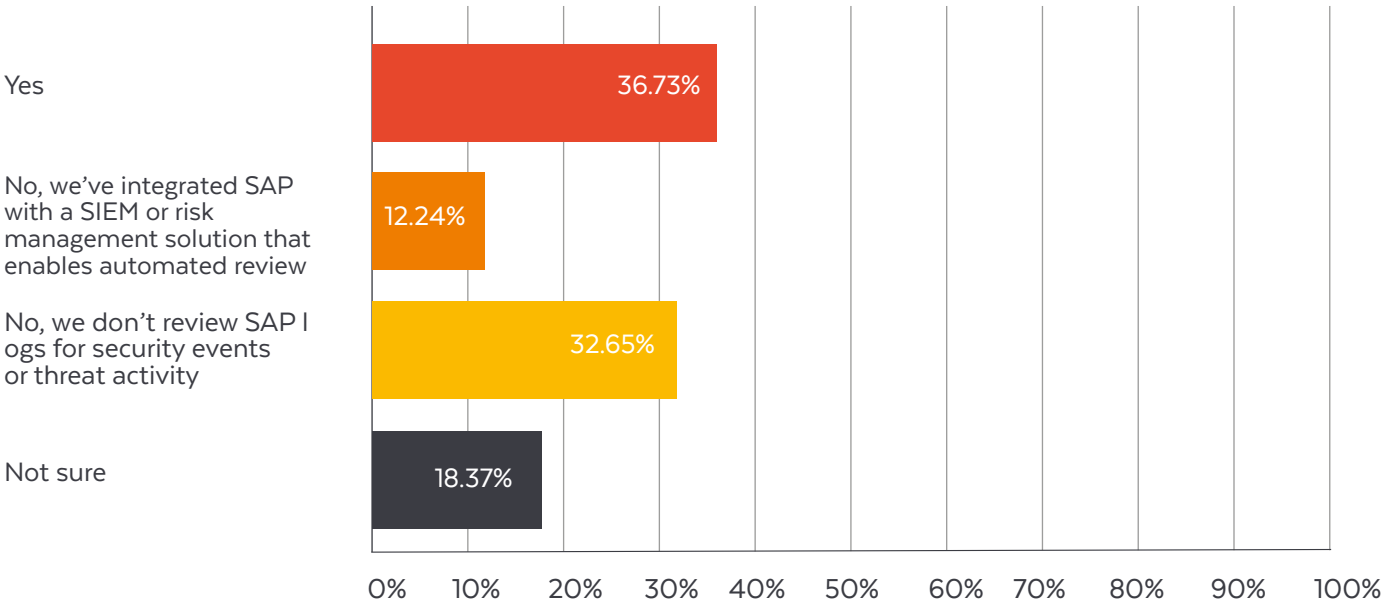
The findings here demonstrate an element of disconnect between SAP security and the wider Security Operations Centers (SOCs) of organisations. Nearly three-quarters of respondents said their SOCs can't see SAP security events, aren't sure if they can, or don't have a SOC. One reason for this disconnect could be that organisations don't want their SOC's time to be taken up investigating false positives that are flagged up as SAP security events.

E: info@turnkeyconsulting.com

ONAPSIS TURNKEY

Q13

Are you currently manually reviewing SAP logs for security events or threat activity?



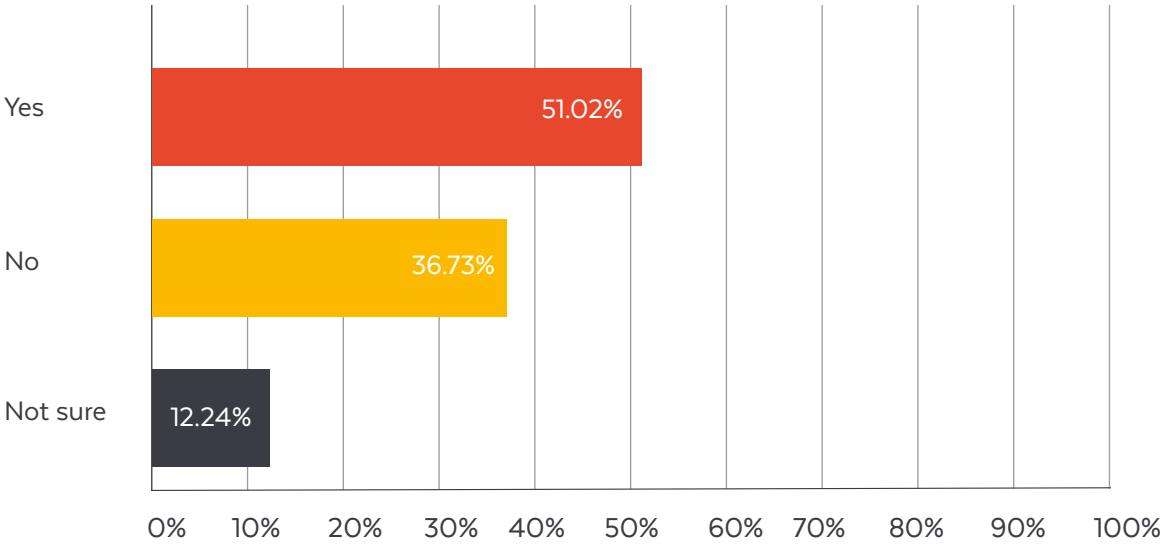
Commentary

Although only one in eight respondents said that they have integrated automated SAP log reviews into a SIEM or risk management solution, this represents encouraging progress in this area. Additionally, while almost a third said they don't review SAP logs for security events or threat activity, it's expected that most are investigating logs when particular issues arise. It's also encouraging that almost half are conducting these reviews, even if many are still doing them manually.

ONAPSIS TURNKEY

Q14

Are your SAP systems always completely up to date and updated with the latest patches?



Commentary

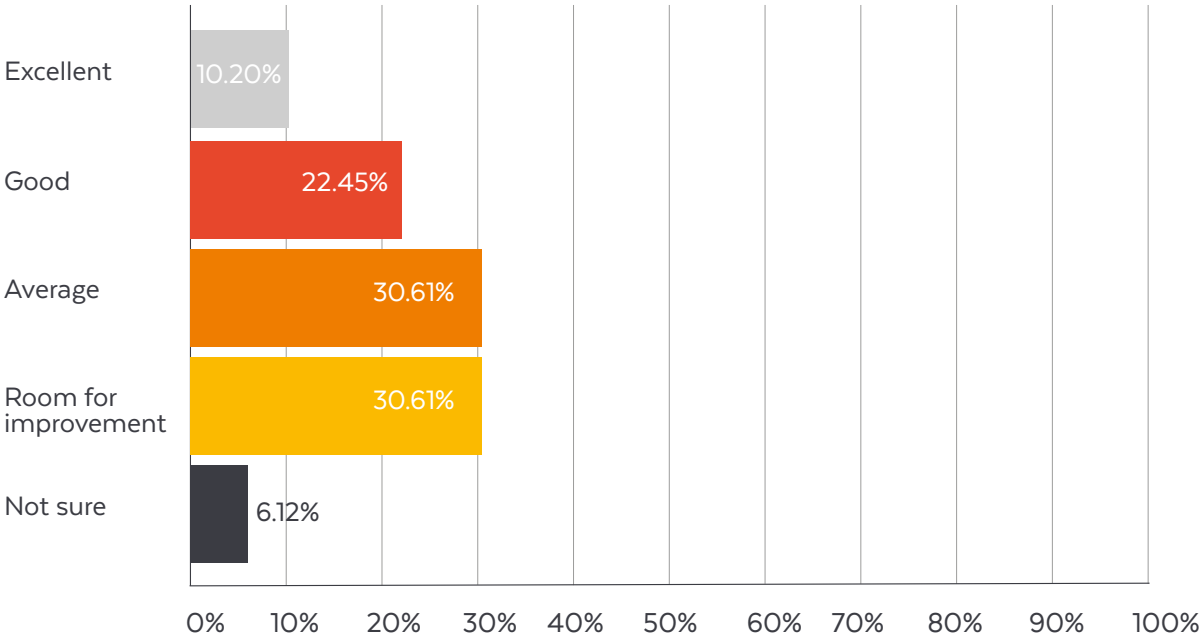
Patches are a vital part of managing and addressing vulnerabilities, so the fact that almost half of respondents couldn't guarantee their SAP systems were always kept up to date is an area of concern. Part of the reason for those who don't keep their systems up to date is that many organisations naturally take some time to apply patches and don't adopt them as soon as they're released. This is due to the need to schedule in downtime when patches can be applied, although these companies are taking a risk as patch vulnerabilities are exploited by cyber criminals increasingly quickly.

E: info@turnkeyconsulting.com

ONAPSIS TURNKEY

Q15

Overall, how would you rate your users' maturity and capability to manage cyber risk to your SAP landscape?



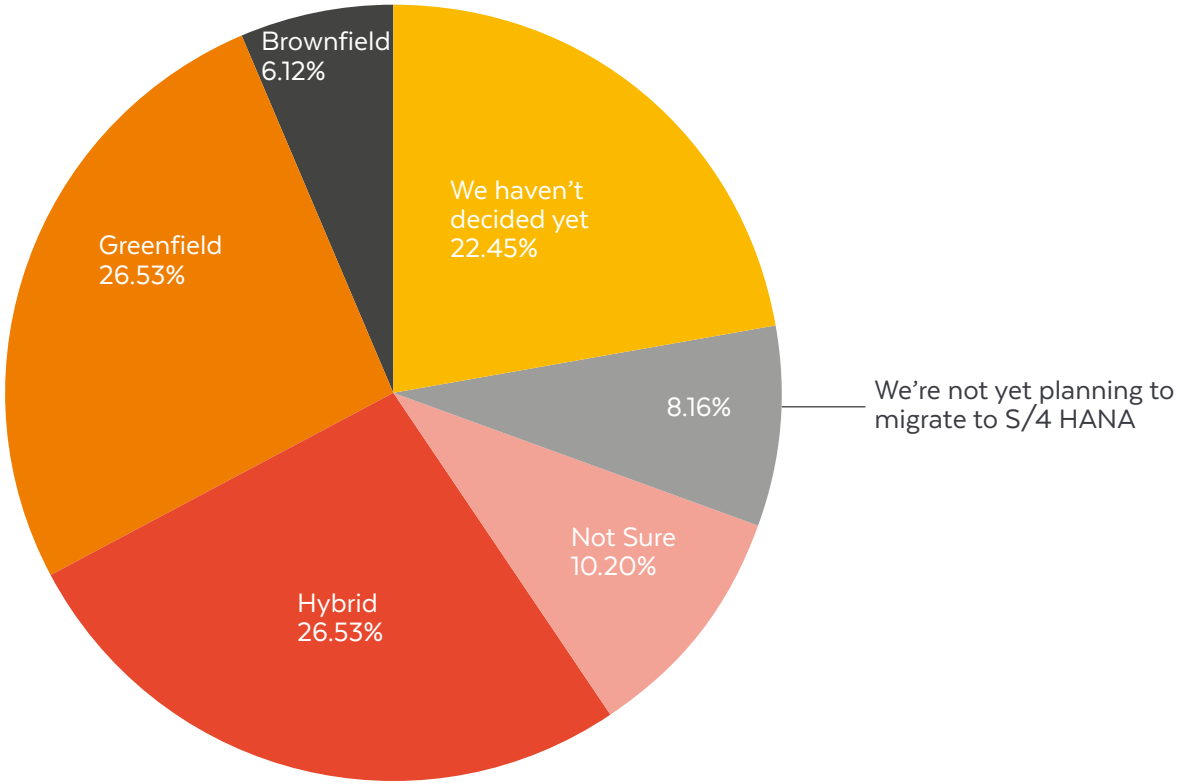
Commentary

As many successful cyberattacks are based around exploiting unsuspecting users, the maturity of those users on an SAP system is paramount, especially with more people working remotely. These results show that there is a broad spectrum of user maturity within respondents, but 60% still feel that their organisations' maturity levels are either average or requiring improvement. That so many respondents have been honest in saying that maturity is not as good as it could be is positive, in terms of the importance of the issue being recognised.

ONAPSIS TURNKEY

Q16

If you are either planning or have already undertaken your migration to SAP S/4 HANA, what type of implementation have you chosen?



Commentary

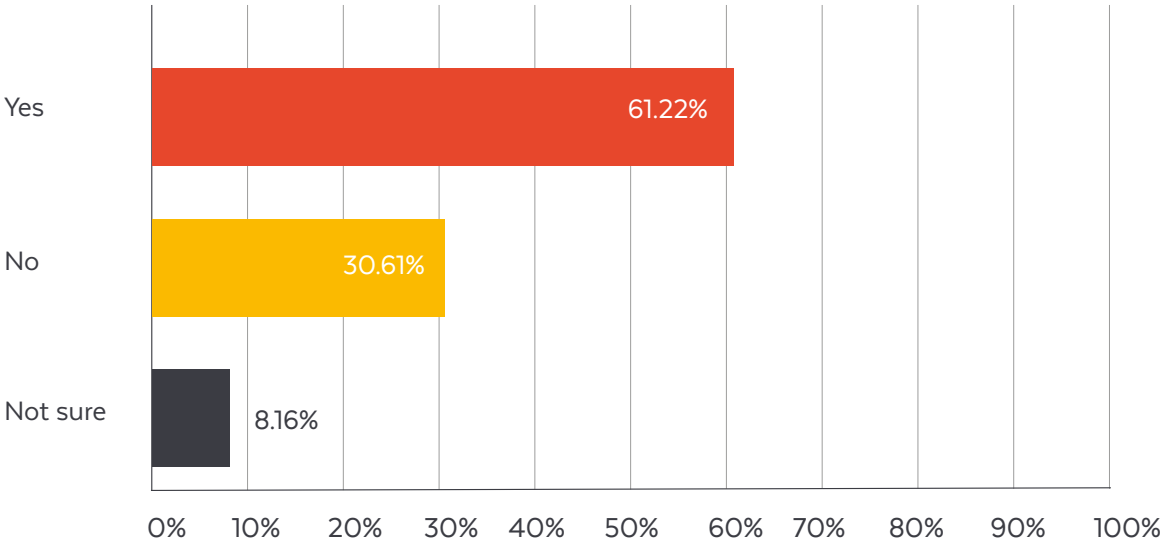
With SAP S/4 HANA giving organisations the chance to enjoy a more interconnected experience, over 80% of respondents have either already migrated to it, or are planning to do so. These organisations are - or will be - moving away from a scenario where SAP sits entirely within their network, and there are knock-on consequences of this change from a security standpoint. However, these organisations can also use the migration as an opportunity to move towards more application-based security initiatives and make long-term security changes for the better.

E: info@turnkeyconsulting.com

ONAPSIS TURNKEY

Q17

Are your SAP systems connected to SaaS applications (e.g., Salesforce, SAP SuccessFactors)?



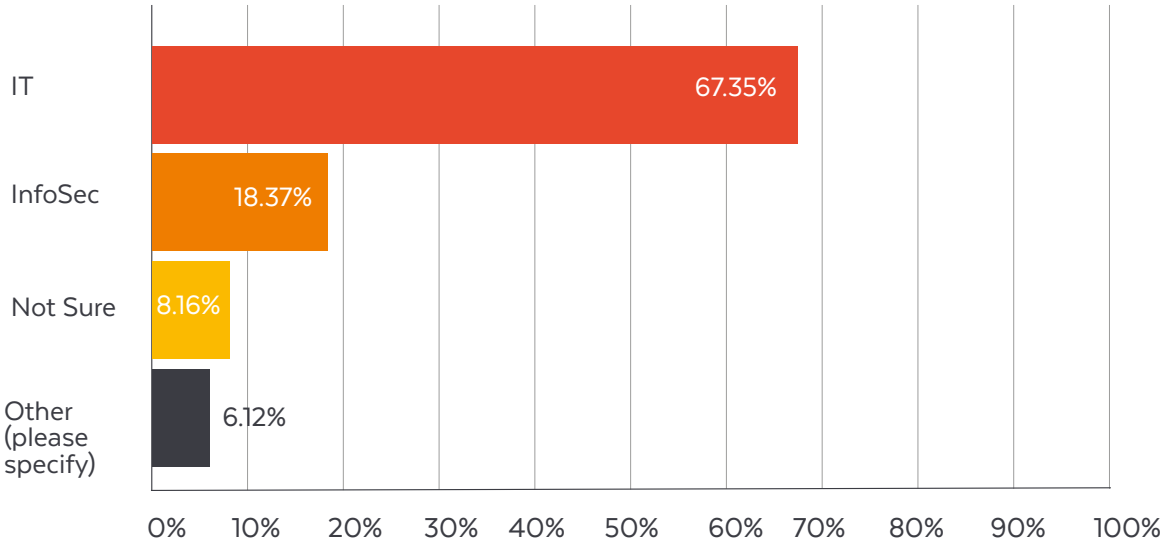
Commentary

As more organisations move towards a cloud-first future, there has been strong take-up of connectivity between SAP systems and Software-as-a-Service applications. However, there are issues around where security responsibility lies when this connection is made: with many cloud providers affirming that it is the customer's responsibility to maintain a strong security posture when using these applications within the cloud.

ONAPSIS TURNKEY

Q18

Who is responsible for SAP application security in your organization?



Commentary

Two-thirds of respondents say that responsibility for SAP application security rests with IT. Part of this is almost by default, where any type of risk - even a business risk within SAP - is automatically assumed to be covered by IT. Low take-up of business areas of these responsibilities is a concern, but this shows there are opportunities to bring ERP and enterprise IT security together so that they work in unison.

E: info@turnkeyconsulting.com

04 Conclusion

The overarching finding of this survey is that many SAP customers are operating under a false sense of security.

Despite the fact that a small majority agree that SAP isn't fully protected within the internal network, the threat from outside is not being taken quite as seriously as it should be.

The risk of this complacency is real and significant. Recent Onapsis research has found that SAP-specific threat actors are active, capable and widespread, and that critical SAP vulnerabilities are being weaponised in as little as 72 hours of a patch being released. The impact of this stretches far beyond the theft of valuable information or the disruption to business, and reaches into compliance implications such as GDPR and SOX.

In order to better protect SAP systems and data, there are four key steps we suggest:

1

Identify risks: assess SAP systems for vulnerabilities, either manually or through automated tools, and remediate any gaps as soon as possible

2

Protect against threats: put a plan in place to protect systems, whether through patching, applying notes, or through monitoring and alerting

3

Detect intrusions and events: use automated solutions to get insight on intruders gaining system access or vulnerabilities being exploited (SAP system information can also be used to inform of these)

4

Respond to breaches: put security incident procedures in place to isolate and deal with attacks without any business process disruption, and with continual patch and vulnerability management of the SAP estate over time

E: info@turnkeyconsulting.com

About Turnkey

Turnkey have a proven track record with regards to security programmes. Our tried and tested methodology facilitates a robust approach within an accelerated timeframe, ensuring a successful outcome feeding into the implementation of solutions and the realisation of associated benefits.

Turnkey's substantial experience performing such engagements mean that common challenges associated with securing systems against risk have been identified and overcome, allowing us to work with you to define strategies which fit to your business and avoid regret costs associated with less integrated and methodical solutions.

Turnkey's global offices:
United Kingdom
United States
Australia
Germany
Malaysia
Singapore
New Zealand

Head Office:
Turnkey Consulting Ltd
58 Ayres Street
London
SE1 1EU

T: +44 (0)207 288 2578
E: info@turnkeyconsulting.com

Integrated Risk Management

Identity & Access Management

Cyber & Application Security

SAP Partner

www.turnkeyconsulting.com