computing
research

RESEARCH PAPER

Out of sight, out of control: How to overcome your IT and OT asset monitoring challenges

January 2022

Sponsored by

ARMIS

CONTENTS

Introduction

IT and operational technology (OT) devices are becoming ever more numerous, diverse, and complex. While this has made organisations more productive and capable than ever before, it has also placed a huge management burden on the technology teams responsible for keeping this environment visible, up to date, and running smoothly. Simply keeping track of the assets you have and their status is a challenge in itself.

The proliferation of connected devices and equipment also puts your organisation at greater risk of cyber security breaches – its increased attack surface offering more entry points to cyber criminals, and a greater risk of security vulnerabilities and outdated software.

Therefore, it’s no surprise that IT and operations leaders across many industries are turning to purpose-built solutions that provide visibility and control across all their IT and OT assets, with the aims of reducing the resource burden of day-to-day management, achieving easier monitoring, cutting downtime, and ensuring more robust security.

This bespoke research examines technology leaders’ current experiences and opinions when it comes to IT and OT asset monitoring challenges. We examine the extent of asset management and monitoring in place and whether that visibility covers different technology areas such as OT and IoT equally. We look at the extent of application of security compliance best practice such as ensuring all devices are running the most up to date software and well supported, network segregation and whether asset registration and risk assessment is undertaken regularly.

Our findings point to a significant gap between beliefs about insight into vulnerabilities and risks generated by sub optimal asset management and the reality in many organisations.

Key findings

- 82 percent expect the number of connected devices/equipment at their organisation to grow in the next three years. 76 percent expect the diversity of these devices to increase and 65 percent anticipate the geographical spread increasing.
- 75 per cent believe that securing these devices will become more challenging, with 69 per foreseeing difficulty managing updates and 57 per cent expecting optimising performance to become more difficult.
- Only 34 per cent have an accurate and up-to-date Asset Management Database of all the assets in their network including IT, IOT, OT, IIoT, and mobile devices.
- Only 40 per cent had identified all devices (including any OT/ICS devices) on their organisation's network.
- The extent of segregation of Operational Technology/Industrial Control Systems device estates from main networks was limited. 39 per cent segregated between none and 20 per cent of their operational systems. A further 17 per cent segregated between 21 and 40 per cent.
- Only nine per cent of organisations stated that none of their estates had fallen out of support or were running end of life software.
- Almost half (48 per cent) said that up to 20 per cent of their devices were running unsupported or end of life software.
- 27 per cent keep a real-time risk register of all assets connected to the network, and 32 per cent had carried out a security risk assessment of IT/OT Infrastructure within the last two months.
- However, 52 per cent believe that they have a good insight into the device vulnerabilities they might have in our IT/OT infrastructure.
- 33 per cent have suffered a security breach in their IT/IoT/OT environment during the last 5 years. A further 16 per cent didn't know if they had.
- Approximately one fifth of respondents (21 per cent) have implemented unified visibility and control of all managed and unmanaged IT, OT, IoT and IIoT devices within their infrastructure. A further 22 per cent are mid deployment.
- For those who have implemented such a solution, satisfaction rates are high, with an average score of 7.4 out of 10 in areas such as hardware monitoring, facilitating remote working, network performance optimisation, reduction in OpEx and improved security compliance.

Impact of the hybrid era on infrastructure management

Fig. 1 : How do you expect the following to change at your organisation over the next three years?

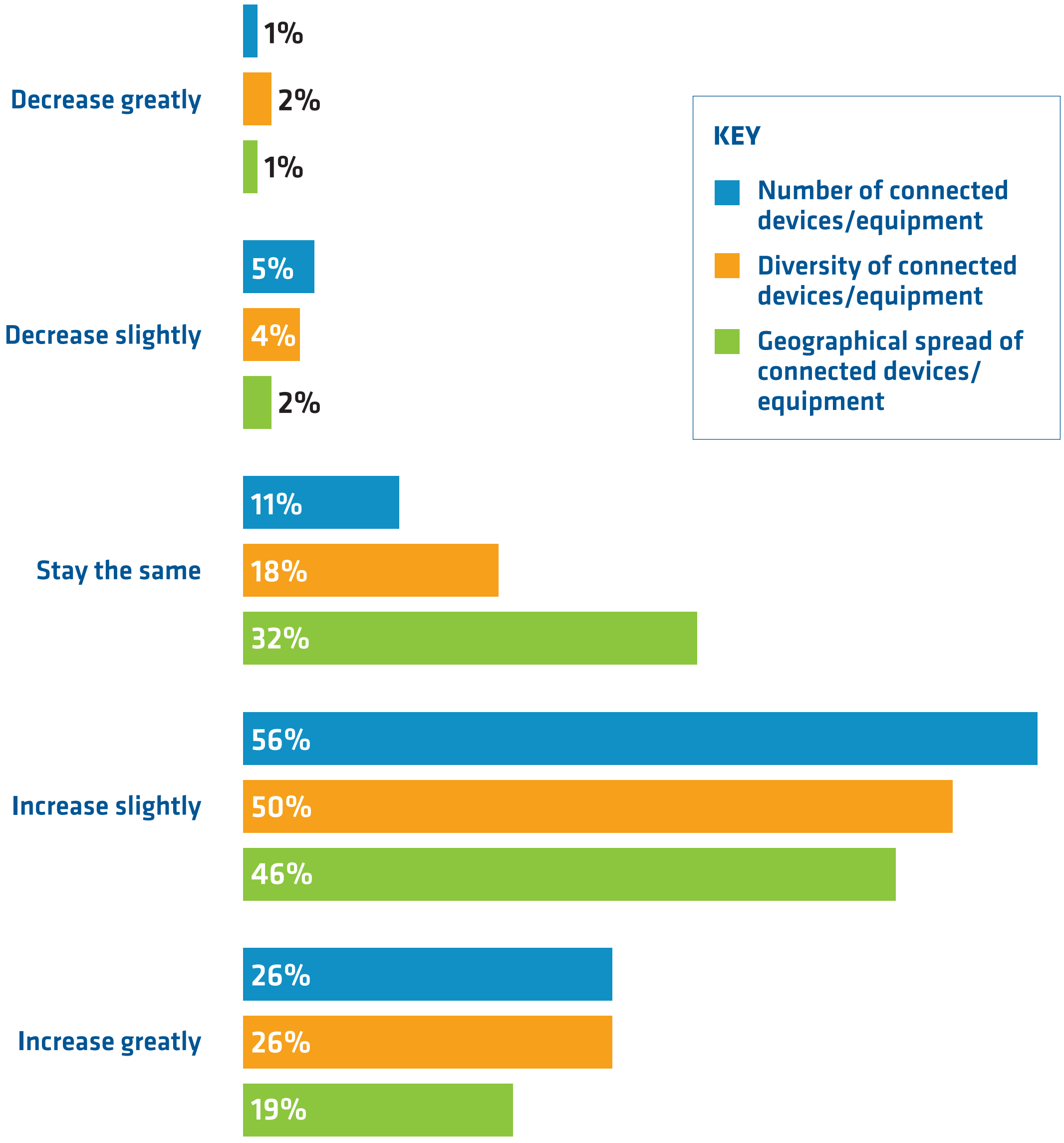


Figure 1 illustrates some of the challenges facing infrastructure teams responsible for the smooth running of technology estates. Issues caused by the sheer number of connected devices, as well as their diversity, have long roots. More flexible and more mobile working has been fuelled *by*, and is fuel *to*, the growing number of cloud and SaaS applications which organisations and their customers use. Cloud growth, along with a more general increase in enterprise mobility, was already causing device numbers to grow before the pandemic.

To add to this complexity, the number of IoT sensors needing to be maintained is also growing significantly, particularly in industries such as transport and logistics, and manufacturing. Indeed, 79 per cent of those questioned agreed to at least some extent that the growth of cloud applications and IoT has redefined infrastructure management.

The pandemic effectively concentrated years of growth in the trends outlined above into a year, and although we all hope the worst of COVID-19 is now firmly behind us, it is clear that the emergence of hybrid working is not merely a passing fad. Reopened offices are not accompanied by expectations of a busy office five days a week. Many organisations are working on a 60/40 split between office and home, and many haven't formally reopened offices at all. Employees have now been freed from their kitchen tables, but many are choosing to split their time between home and other local venues with space to work. This all means that the number, diversity and geographical spread of devices which have to be managed and maintained is not likely to decrease anytime soon.

Fig. 2 : How do you expect the challenge of achieving the following to change at your organisation over the next three years?

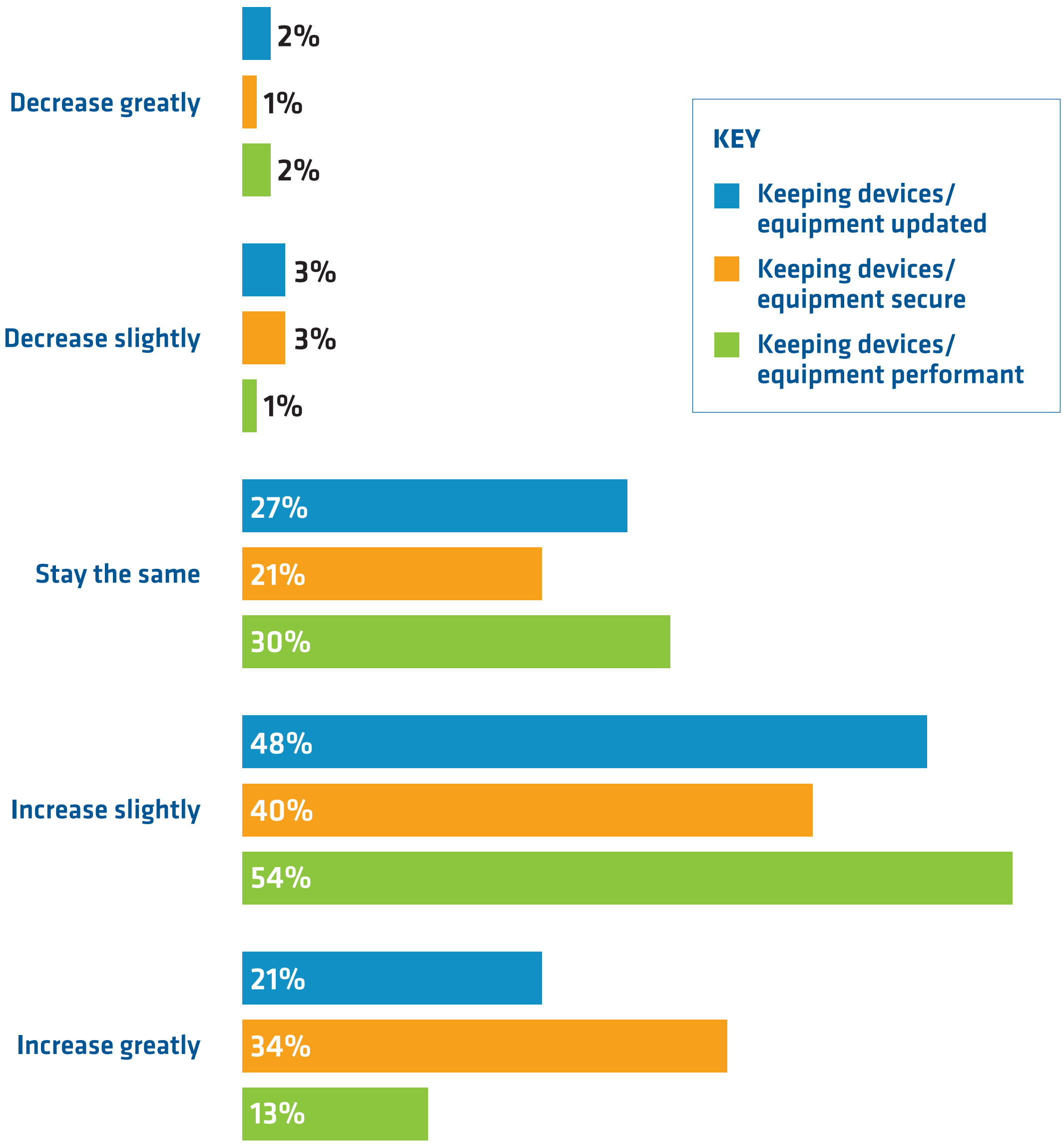


Figure 2 gives an indication of the impact of these trends. Three quarters of those taking part in our research told us that they expected the challenge of keeping this plethora of devices secure was likely to increase to at least some extent, and 34 per cent expected it to increase greatly. Only slightly fewer (69 per cent) thought that managing updates was going to get more difficult, and 57 percent were concerned about optimising performance. In truth, these challenges are all linked. A device which is not carrying the latest security updates is not going to be secure, and this is likely to have detrimental impact on performance.

Visibility, segregation and the importance of updates

Our researchers were keen to broaden out the discussion to include not just traditional IT systems used by employees on and out of offices but also industrial systems including Operational Technology (OT) and Internet of Things (IoT.) They asked those participating the extent to which a number of statements were true for their organisation. The results of this exercise indicate that organisations have seriously compromised visibility of the assets for which they are responsible and that this is having a damaging impact on security. The statements and proportion of respondents stating that they were true for their businesses were as follows:

44% said

“We have insight into all the network connections in our infrastructure and how traffic flows.”

40% said

“All devices (including any OT/ICS devices) on the organisation’s network have been identified.”

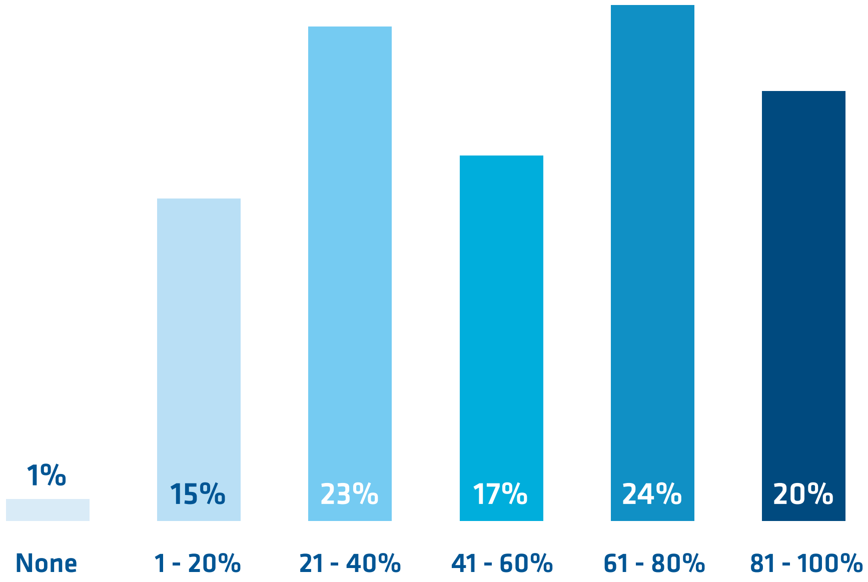
34% said

“We have an accurate and up-to-date Asset Management Database of all the assets in our network (IT, IOT, OT, IIoT, mobile devices.”)

These answers suggest that a majority of organisations are fighting to maintain even partial visibility of their IT and OT assets. To drill down further into the issue of visibility, we asked respondents the proportion of their devices that they believed they had visibility of, and the answers are shown in Figure 3. The fact that so many of the organisations taking part in our research openly admit that they do not have visibility of almost half of the devices that can access their networks is both surprising and a cause of concern.

Many organisations segregate their networks, with OT being separated from IT estates, and/or IoT being completely separated from main networks. Segregation is put in place to reduce risk. The huge risk in connected devices arising from IoT, for example, poses a threat to corporate cyber security as a whole, so it makes sense to segregate it. Equally, separating IT from OT means that in the event an office worker being compromised with ransomware, the attack doesn’t spread to operational systems and take out manufacturing systems. A well planned and maintained network segregation can play a big role in damage limitation and therefore the mitigation of ransomware and other types of malware.

Fig. 3 : What percentage of your unmanaged devices do you believe you currently have visibility of?



We asked respondents approximately what percentage of their Operational Technology/Industrial Control Systems device estate was segregated from their main networks? The answers varied but tended to a much lower proportion than we might expect given the fact that segregation would be considered good practice. 39 per cent segregated between none and 20 per cent of their operational systems. A further 17 per cent segregated between 21 and 40 per cent. Only 13 per cent segregated between 80 and 100 per cent of their operating systems.

The bad news doesn't stop there. Another plank of best security practice is to ensure that device estates are running the most up to date software versions with all of the necessary security patches applied. It should go without saying that versions should be supported by manufacturers in order to ensure that issues can be promptly resolved.

In fairness, versions often have to be several old before vendors stop supporting them. Microsoft won't stop supporting Windows 10 until 2025 – a good 4 years after the recent release of Windows 11. However, only 9 per cent of organisations represented could say with confidence that none of their estates had fallen out of support or out of date. 48 per cent said that up to 20 per cent of their devices were running unsupported or end of life software, with a further 22 per cent saying it could be up to 40 per cent of their estates.

Impact on risk

The combination of poor visibility of devices, limited network segregation between different categories of technology, and the amount of out of date or unsupported systems reported by those participating in our research suggests that many organisations are running some substantial – and wholly unnecessary – risks. An impressive 85 per cent agreed either somewhat or strongly that "ineffective remote IT/OT management presents a cyber security risk to organisations." Almost the same proportion of respondents agreed that this cyber security risk translates directly into financial risks. 83 per cent agreed that "ineffective remote IT/OT management presents a financial risk to organisations."

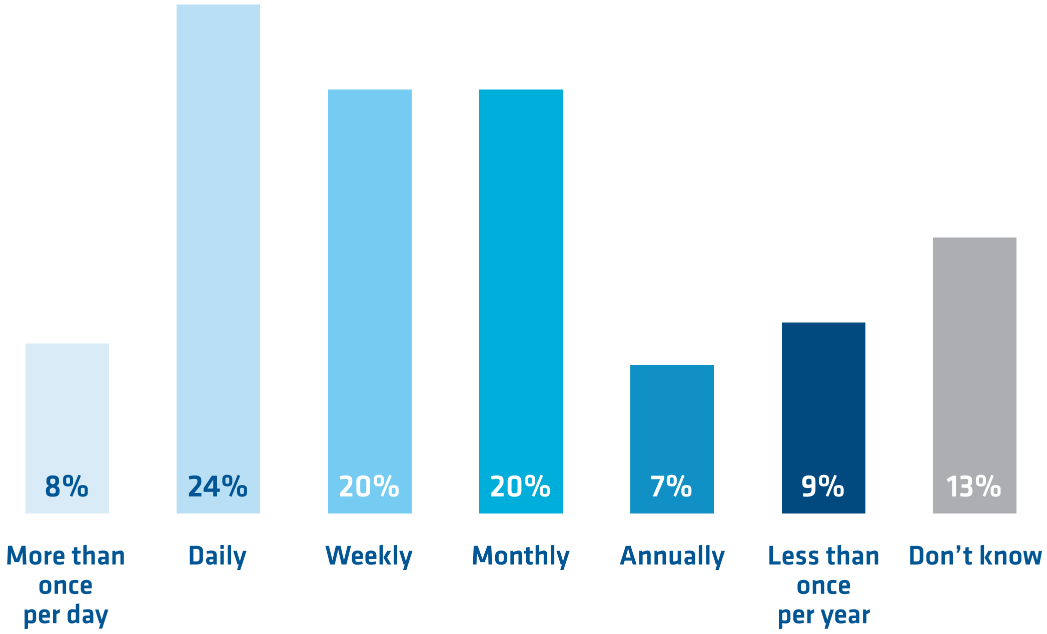
However, it is only a minority of organisations that keep a risk register of corporate IT/OT assets, and regularly assess the risk that these devices pose. Only 27 per cent keep a real-time risk register of all assets connected to the network, and only 32 per cent had carried out a security risk assessment of IT/OT Infrastructure within the last two months.

Interestingly, 52 per cent said that they have a good insight into the device vulnerabilities they might have in our IT/OT infrastructure. Given such limited visibility of assets the question arises – how can they be so confident?

These findings look all the more alarming when considered in the light of the barrage of malware, particularly ransomware attacks that organisations of all kinds are presently being subjected to. Attack volumes have escalated this year and the nature of attacks has also changed. Ransomware moves laterally through business networks, hunting out backups before victims identify the attack. Cyber criminals are taking advantage of the typical complexity and geographical spread of enterprise networks to exploit a target that is growing all the time.

Figure 4 illustrates the frequency of attacks, with more than half of those participating (52 per cent) stating that they see attacks either weekly or more frequently. The fact that 13 per cent didn't know how often they were attacked is an indicator of seriously compromised infrastructure visibility and monitoring for these organisations.

Fig. 4 : How frequent are genuine cyber security attacks against your IT/IoT/OT environment?



When asked, **"have you had any security breaches in your IT/IoT/OT environment during the last 5 years?"** 33 per cent replied yes. 51 per cent said no with the remaining 16 per cent unsure.

These figures strongly suggest that criminals are successfully exploiting the commonly occurring combination of obscured asset visibility, slowness to update operating systems and a lack of network segregation.

Conclusions

The findings of our research into the visibility, control and security of IT and OT assets are cause for concern. As hybrid working becomes the norm and IoT deployments scale up, the number and variety of devices which have to be tracked, managed and secured is growing fast. A large majority expect the task of managing updates, optimising performance and securing these devices to get harder in the next few years.

Enterprises are being hampered by poor visibility of assets. Barely a third of the organisations represented were confident that they had an accurate and up-to-date asset management database of all the assets in their network, including IT, IoT, OT and mobile devices. Furthermore, the segregation of OT and ICS technology from main IT networks was also limited in scope. Perhaps most worrying of all was the fact that only nine per cent believed that none of their technology estates were built on unsupported or end of life software.

This combination is presenting a serious risk to enterprises. One third admitted to having incurred a cyber security breach within the last five years. However, scarcely more than one quarter (27 per cent) of participants said that they keep a risk register of corporate IT/OT assets.

Our research has demonstrated why enterprises need to get on top of their growing mountain of assets and shown how far many of them have to travel to do so. However, some of those we spoke to had already implemented a solution which provided unified visibility and control of all managed and unmanaged IT, OT, IoT and IIoT devices within their infrastructure. 21 per cent had already implemented a solution and a further 22 per cent were in the midst of rolling one out. 18 per cent were in the incubation/trial stage.

When those who had installed such a solution or were doing so were asked to rank their top three motivations for pushing ahead with this project the top priority by a significant margin was to improve security compliance. To provide an illustration of just how important security is as a motivator, it is worth stating that 42 per cent of those responding flagged it. The second most highly scoring motivator was the need to reduce IT team workload which, for comparison, was chosen by 26 per cent. Ranked third on 23 per cent was the facilitation of and reaction to increased remote working.

Fig. 5 : On a scale of 1 (not at all successful) to 10 (extremely successful) how successful has the implementation of unified infrastructure visibility and control capabilities been in achieving these motivations?

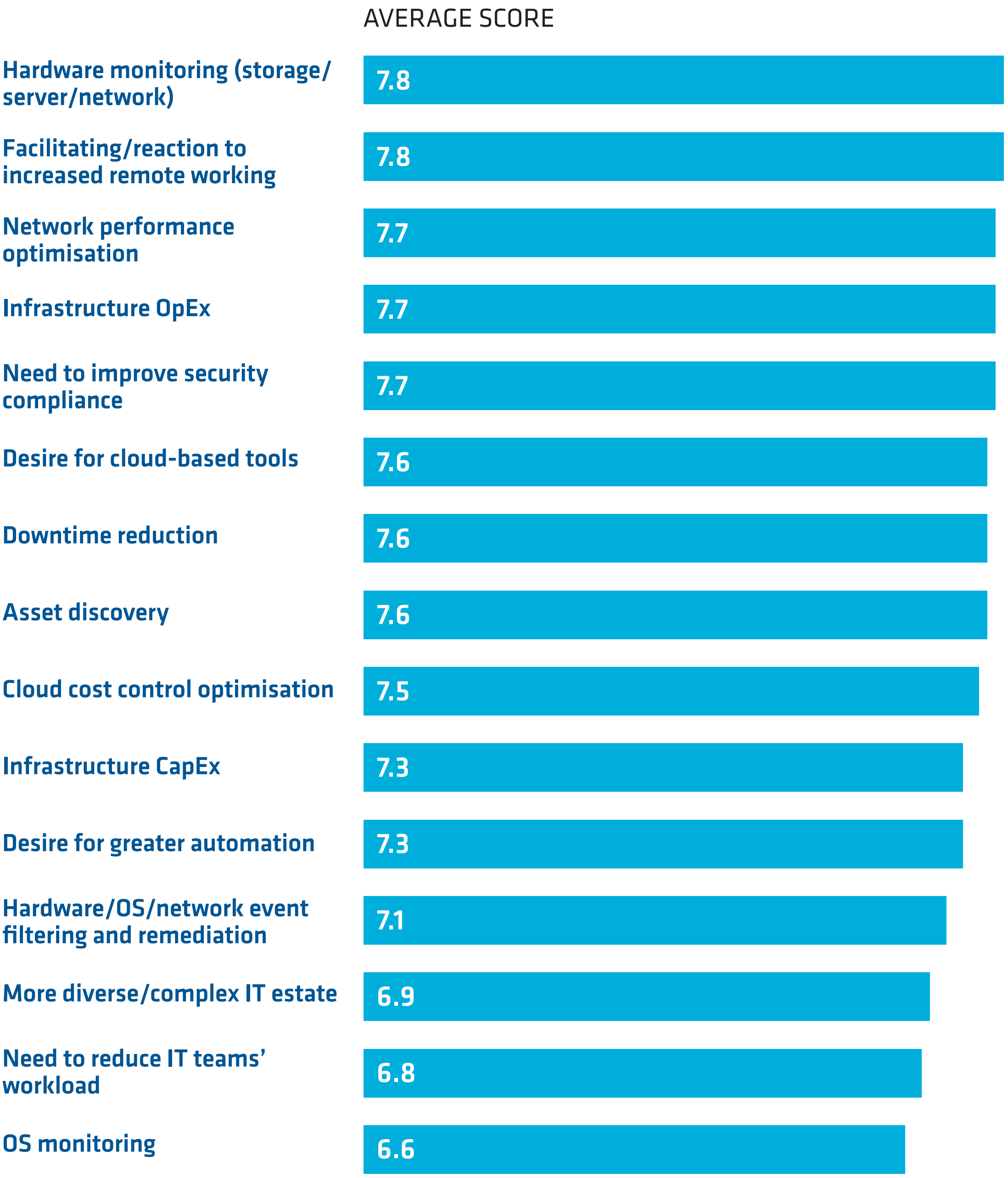


Figure 5 shows how well centralised asset management is performing. Across all categories, the average score was 7.4 out of a possible 10 which indicates that these solutions are delivering what they promised. The differences in scoring between areas like hardware monitoring and improving security is incredibly marginal, with less than a tenth between many of the higher scoring attributes.

From the list above we can see that where centralised asset management with a high degree of autonomy is place, organisations are not only optimising the performance of their IT and OT assets, but the centralised visibility is leading to an improved security posture and a reduction in the costs of maintaining devices, as well as a reduced burden on infrastructure teams who can be refocused in a more strategic direction. Indeed, 83 per cent of those we surveyed agreed that automated infrastructure management has a key role to play in augmenting IT teams today.

81 per cent agree that unified visibility and control of IT and OT assets are now a must have, yet only a minority do so – despite near universal interest. Our research has uncovered a clear gap between aspirations and reality. In order to optimise their technology assets to compete in the digital economy, and reduce the risks and costs that they're exposed to, enterprises must have a centralised view of all of their technology assets, and a degree of automation, that ensure that all devices are up to date, patched and within the support terms of manufacturers. The financial, reputational, and operational costs of not doing so can be extremely difficult to recover from.

About the sponsor, Armis

By 2025, there will be 41.6 billion connected devices and 90% of all these devices are unmanaged. These unmanaged devices cut across all sectors including printers and card readers in Enterprises, security cameras and robots in Manufacturing, even MRIs and blood infusion pumps in Healthcare. The exponential increase in the number of these devices are hard to identify and secure, providing an ever-expanding attack surface for malicious actors to exploit to disrupt production, impact patient care, or result in financial loss.

These devices, often referred to as the Enterprise of Things devices, Internet of Medical Things (IoMT), the Industrial Internet of Things (IIoT), or just the Internet of Things (IoT), were not designed with IT security or management in mind and cannot be protected in the same manner as traditional devices. This makes them valuable targets for malicious exploitation.

Armis is the leading unified asset visibility and security provider designed to address the new threat landscape that diverse connected devices create. Armis discovers every managed and unmanaged IT, OT, IoMT and ICS devices. Uniquely Armis analyses device behaviour to identify risks or attacks and protects critical business information and systems in an agentless manner with its global Knowledge Base of 1 billion device profiles and patterns. Companies trust Armis to provide passive and unparalleled cybersecurity asset management, risk management, and automated enforcement to keep them safe and secure from cyber criminals.

Welcome to the new world of 100% asset visibility. SEE EVERY ASSET. EVERY CONNECTION. EVERY THING.

To learn more:

Visit: www.armis.com/armis-platform

ARMIS™

Appendix: The research participants

The survey respondents were made up of 149 decision-makers involved in using, testing, evaluating or procuring IT/OT infrastructure management products at their organisation, across a range of industries and company sizes.

Fig. 6 : Job roles

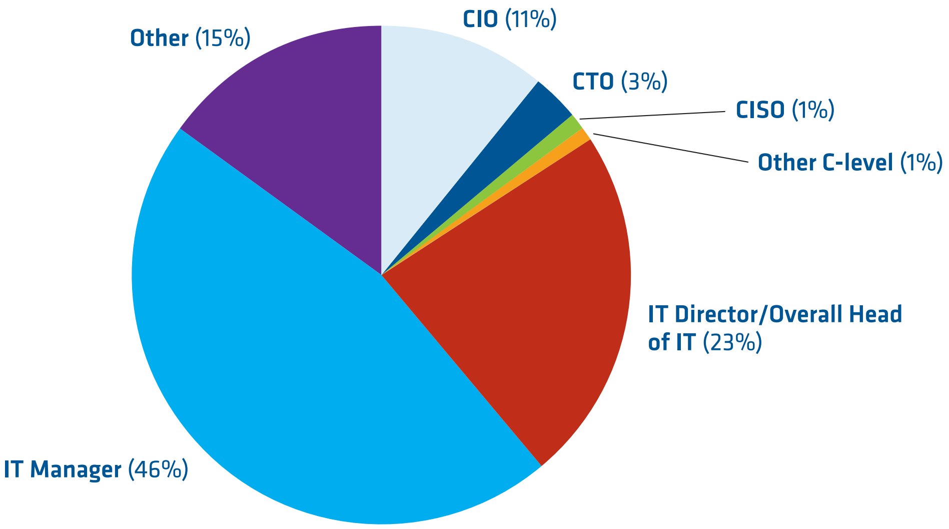


Fig. 7 : Number of employees

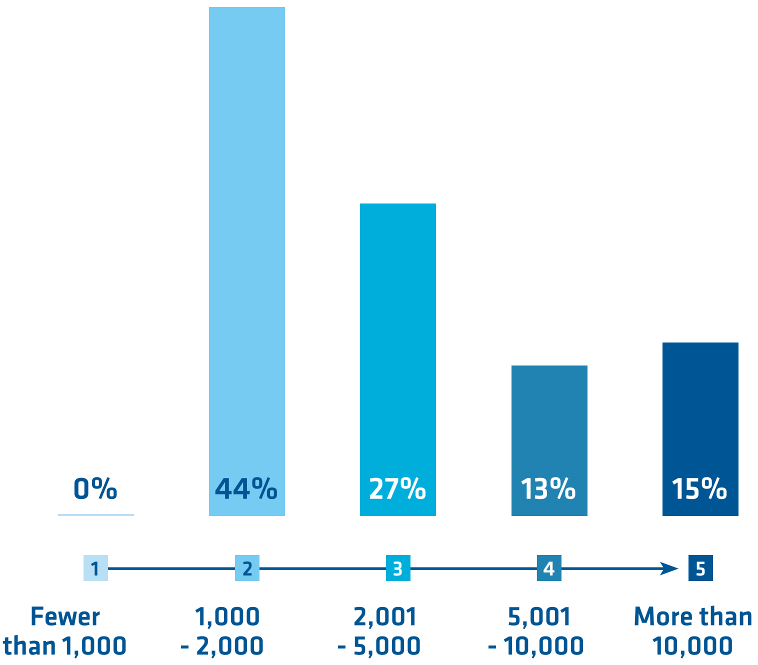
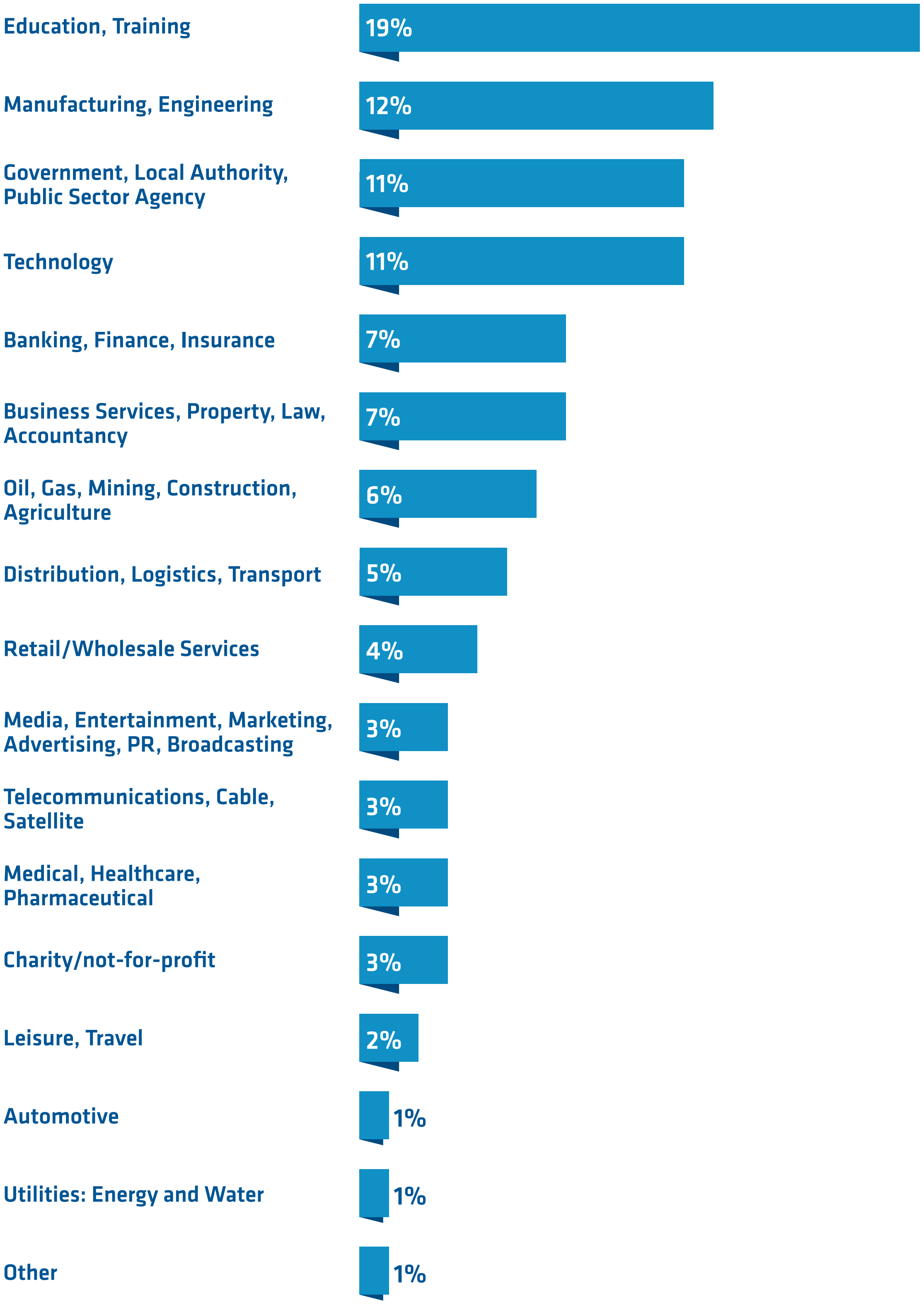


Fig. 8 : Vertical sector


Education, Training
Manufacturing, Engineering
Government, Local Authority, Public Sector Agency
Technology
Banking, Finance, Insurance
Business Services, Property, Law, Accountancy
Oil, Gas, Mining, Construction, Agriculture
Distribution, Logistics, Transport
Retail/Wholesale Services
Media, Entertainment, Marketing, Advertising, PR, Broadcasting
Telecommunications, Cable, Satellite
Medical, Healthcare, Pharmaceutical
Charity/not-for-profit
Leisure, Travel
Automotive
Utilities: Energy and Water
Other