IFF Research

Enterprise connected devices: procurement, usage, and management among UK businesses

19 October 2021

Contents

1 Executive summary

The Department for Digital, Culture, Media and Sport (DCMS) commissioned IFF Research to carry out a telephone survey among UK businesses to understand how businesses procure, deploy and manage enterprise connected devices. This includes both consumer and enterprise-grade devices, used within their organisational networks. This research was undertaken to help inform DCMS's development of policy interventions.

The quantitative survey was developed in collaboration with DCMS and refined after two pilot fieldwork phases to increase uptake among participants. Fieldwork took place between Monday 7th June and 4th August 2021. A total of 124 interviews were completed with IT and cyber security professionals in medium (50-249) and large-sized businesses (250+ employees), among five sectors: retail, research and development, finance and insurance activities, healthcare, and transportation and storage. The participants interviewed held a range of roles, often within the remit of IT or operations, such as: Chief Technology Officer, (Senior) IT manager / IT network supervisor, Operations director / Senior director, Business unit manager, and Facilities manager.

The definition of connected devices for the purposes of this research was provided to participants in the survey introduction and at the start of each topic during the interview. There is evidence to suggest that some participants may have been confused by the definition of connected devices and may not have considered all devices in scope. For example, 15 businesses reported that they had fewer than 50 connected devices in use, which would mean that not all staff members in businesses of at least 50 employees had access to their own commonly used business device such as a desktop or laptop computer, VoIP telephone, or a smartphone. It is likely that these participants did not consider such everyday devices in their responses and under-reported the scale of devices in use within their network. In addition, and as discussed further in Chapter 6 'Management of connected devices within organisational networks', only one business interviewed reported they had experienced a cyber-security attack as a result of their use of connected devices, far lower than the proportion reported in the Cyber Security Breaches Survey 2021[9] (DCMS, 2021).

Participants were reassured that taking part in the survey was on an anonymous basis and the findings would not be reported in a way that could identify their business. Despite this, and given the sensitive nature of the survey topics, it is possible that some participants may have chosen not to report the full extent of their business' usage, procurement, and management of connected devices.

A summary of the key findings is presented in the following paragraphs.

Businesses reported a wide range of connected devices used within organisational networks, ranging from 6 to 50,000 devices. Over two-thirds (36%) of large businesses used over 1,000+ devices within their network, whereas just 1% of medium-sized businesses used connected devices at this scale. Among medium-sized businesses, the average number of devices in use was 185, while for large-sized businesses this figure was significantly greater with 2,949 devices in use.[1]

When asked whether they keep track of the number of devices deployed within organisational networks, most businesses (93%) said that they keep track either internally (81%) and/or through their suppliers (20%). Businesses with 100 or fewer devices in use were significantly more likely to

[1] This analysis is based on businesses who told us the exact number of employees within their organisation. Two medium and two large-sized businesses did not provide this information and are not included in the average score calculations.

only rely on their suppliers to keep track of potential threat vectors (28%), compared to businesses that deployed between 101-250 devices (9%) and those that deployed 250+ devices (2%).

In terms of monitoring potential threat vectors for the devices currently in use, around three-quarters (76%) of businesses reported that they keep track of the potential threat vectors for the devices connected to their network, either internally (44%) or both internally and through their suppliers (32%). Businesses who said they keep track of threat vectors were asked to state in their own words how they keep track. A range of responses were given yet there was no common approach. Around one in five (21%) said they used some form of monitoring or anti-virus software but did not mention the specific product name; just 13% provided the specific monitoring or anti-virus product name when asked to state how they track of potential threats. A further 14% said they carried out real time monitoring, and 10% used threat intelligence platforms, while 7% each used regular systems testing and firewalls.

In addition, businesses varied in how frequently they conducted a risk assessment of threats posed by their use of connected devices, around one-third (35%) carried out a risk assessment at least monthly, while just over one-quarter each carried out an assessment bi-annually (26%) and annually (27%).

In advance of purchasing new devices, over half (58%) of businesses said that their organisation does not require any security and procurement checks to be undertaken. One-third (33%) of businesses said that checks were required.

When asked about the type of cyber-insurance policy they have in place, around one-third (32%) of businesses said they do not know whether their organisation has a cyber security insurance policy. Just under half of businesses (48%) said they do have cyber security insurance, either as part of a broader insurance policy (26%), or as a standalone policy (21%). Among businesses who have cyber security insurance, around one-quarter (26%) did not know whether the policy covers cyber security attacks stemming from their use of connected devices and two-fifths (42%) also did not know whether their insurer offers any discounts based on taking specific security actions.

Businesses with cyber-security insurance cover reported that there are a range of security actions requested under their insurance policy, however there was no unifying theme. This suggests that there is no common approach from insurers in terms of taking mitigating action against cyber security attacks in relation to the use of connected devices, as set out in their insurance policies. The most common security action, requested from 40% of businesses, was to carry out regular penetration tests. Around one-third of businesses each said that employees must take cyber security training (31%) and to ensure that only connected devices that conform to particular security standards are procured (30%). One in four (25%) businesses each said the organisation must have Cyber Essentials certification while one in five businesses (19%) are required to have industry certification or meet international standards, such as ISO 27001. One in four (25%) businesses said that there are no such requirements in their insurance policy, and 12% said they did not know what actions were requested.

2 Introduction

Background

The Department for Digital, Culture, Media and Sport (DCMS) commissioned IFF Research to conduct a survey of IT and cyber security professionals to understand how UK businesses procure, use and manage connected devices within their organisational networks.

Connected devices refer to objects which communicate with each other and with the internet and wider systems via either wired or wireless connections; popularly referred to as the 'internet of things' (IoT). The use of such devices has become increasingly common in the home, including smart TVs and other appliances, home security systems and routers.

Connected devices are now also increasingly used in business settings, where they offer many benefits in terms of connectivity, efficiencies, and data analysis. Alongside the benefits, the use of connected devices within businesses also brings potential risks, particularly for larger businesses. These devices can act as entry points into businesses' systems for hostile actors able to exploit security vulnerabilities. Such vulnerabilities could include poor password controls and management, a lack of security updates, and insecure ways of accessing a device over an organisational network. It was in this context that DCMS commissioned IFF Research to carry out primary research among UK businesses.

Research objectives

For the purposes of this research, 'connected devices' has been defined as:

"Devices that serve a business function, such as laptops, desktop computers and printers but NOT medical, operational or industrial equipment (such as Industrial Controls Systems, often referred to as ICS or 'SCADA'). Other connected devices of interest include: Smartphones, video conferencing systems, room booking systems, and network attached storage devices (NAS). Any consumer grade devices used in the business setting, such as smart TVs, music speakers, voice assistants etc."

The core objectives of the research were to understand and explore the following:

- To understand businesses' attitudes when using connected devices, such as:
    - Responsibility within the organisational structure when purchasing, managing, or auditing connected devices
    - Awareness of existing cyber security threats and mitigations for connected devices
    - The role of cyber insurance in managing risk for enterprise connected devices
- To understand the organisational, technical, and logistical processes by which businesses typically procure, deploy and manage connected devices.
- To highlight the resources and processes that businesses use and complete to stay updated on evolving cyber threats

Survey fieldwork

This report is based on data from a quantitative telephone survey comprising of 124 interviews conducted with UK businesses between June and August 2021.

Data analysis and data weighting

Analysis by business type such as size and sector has been carried out and is referred to in this report where it is statistically significant and relevant. Significance tests indicate how likely it is that a pattern seen in data is due to chance or not, and therefore how likely it is that it is a genuine difference between the groups being compared. All differences noted in this report are significant to a 95% confidence level: by convention, this is the accepted statistical 'threshold' used to determine whether an observed difference is large enough to be regarded as real. This means the significant differences noted throughout this report have a 95% chance of being 'true', i.e. due to a genuine difference in the groups being compared, and only a 5% chance that the results are just due to chance.

Any sub-group differences between sectors should be considered indicative only due to the low base sizes. In charts, where there is a statistically significant change between sub-groups, these are marked with arrows reflecting the direction of change (e.g. positive or negative). For multi-response questions, the sum of the total responses may exceed 100%. This is because a business could provide more than one response, and responses are not mutually exclusive. For single-response questions, the sum of all responses may not add up to 100% due to rounding. For example, a response may represent a percentage of 65.54% and this will be rounded up to 66%.

Survey data has been weighted to ensure that the results are reflective of the population of in-scope UK businesses according to industry sector and number of employees. The weighting profile was based on the 2020 Business Population Estimates (BPE) (Department for Business, Energy & Industrial Strategy, 2020).[2]

[2] Department for Business, Energy & Industrial Strategy, 2020. "Business population estimates for the UK and regions 2020", https://www.gov.uk/government/statistics/business-population-estimates-2020

3 Methodology

A quantitative survey was developed in collaboration with DCMS and refined during two pilot fieldwork phases. Interviews lasted an average of 25 minutes and fieldwork was conducted using Computer Assisted Telephone Interviewing (CATI) between Monday 7th June and 4th August 2021 (inclusive of the pilot fieldwork phases). Telephone interviews were carried out with the person responsible for the management of connected devices within the organisation. To aid the receptionist or call-handler in progressing the interview request, the interviewing team initially asked to speak to the 'Head of IT' or 'IT department', and from here the most appropriate individual was identified.

Participants interviewed held a range of roles, often within the remit of IT or operations, such as: Chief Technology Officer, (Senior) IT manager / IT network supervisor, Operations director / Senior director, Business unit manager, and Facilities manager.

Sectors of interest and interview targets

This research initially sought to interview a total of 400 businesses, split equally among five sectors (retail, research and development, finance and insurance activities, healthcare, transportation and storage) with a focus on larger businesses (250+ employees). As a result of significant challenges experienced in securing interviews with businesses, interviewing targets were refined to be on a 'best effort' basis. The sectors were chosen based on evidence from previous DCMS research which highlighted that these sectors were either most at risk from vulnerable devices or the sectors reportedly had the most connected devices on their network. DCMS's research was focused on companies, therefore only private healthcare companies and pharmaceutical manufacturing were included within the healthcare sector sample.

The sectors of interest for this research and the corresponding SIC[3] codes (Office for National Statistics, 2007) are shown in Table 3.1 below.

Table 3.1 Sectors of interest

Sector	Two-digit SIC codes
Retail	47 - Retail trade, except of motor vehicles and motorcycles
Research and Development	62 - Computer programming, consultancy and related activities 72 - Scientific research and development
Finance and Insurance activities	64 - Financial service activities, except insurance and pension funding 65 - Insurance, reinsurance and pension funding, except compulsory social security 66 - Activities auxiliary to financial services and insurance activities
Healthcare	21 - Manufacture of basic pharmaceutical products and preparations 86 - Human health activities
Transportation and storage	49 - Land transport and transport via pipelines 51 - Air transport 52 - Warehouse and support activities for transportation 53 - Postal and courier activities

[3] Office for National Statistics, 2007. UK Standard Industrial Classification of Economic Activities 2007 (SIC 2007).

Sample

The sample for this survey was predominantly sourced from Market Location, a commercial database of UK businesses. The 'sample to interview' ratio was initially predicted to be 12:1, based on other research with business audiences. However, soon after the launch of the pilot, it became apparent that it was significantly more challenging to first speak to an individual within the IT team and then to identify and secure an interview with the individual responsible for the management of connected devices. These issues are explored in the following section "Recruitment challenges".

Achieved interviews and response rate

Profile of participating businesses

A total of 124 interviews were achieved, split by size and sector in Table 3.2 below.

Table 3.2 Profile of participating businesses (achieved interviews)

Sector	Business size		
	Medium (50-249)	Large (250+)	Total
Retail	19	3	22
Research and Development	18	13	31
Finance and Insurance activities	13	5	18
Healthcare[4]	10	5	15
Transportation and Storage	26	12	38
Total	**86**	**38**	**124**

The data was weighted to reflect the actual proportions of in-scope UK businesses according to industry sector and size,[2] as shown in Table 3.3.

Table 3.3 Profile of participating businesses (weighted)

Sector	Business size		
	Medium (50-249)	Large (250+)	Total
Retail	30	2	32
Research and Development	19	7	26
Finance and Insurance activities	17	3	20
Healthcare[4]	13	3	16
Transportation and Storage	22	6	29
Total	**102**	**22**	**124**

[4] Businesses interviewed in the Healthcare sector included private healthcare companies and pharmaceutical manufacturing only. NHS provision as well as private medical centres / care homes were excluded.

Call outcomes and survey response rate

A call outcome is defined as a definite response to the survey invitation, i.e. whether an interview was achieved, or whether an interview could not be achieved and the reason was established. Among the 5,601 businesses called at least once, the response rate for the survey was 2%. This included businesses where no final outcome was reached, for example where the interviewing team were not able to get through to the right person, where an appointment had been made to call back at a later date, or where a or where the call went to answerphone. Among the 2,158 businesses where a definite call outcome was achieved (n=2,158), the response rate was 6%.

The 'sample to interview' ratio among businesses called at least once was 45:1, and 17:1 among businesses where a definite call outcome was reached.

For just over half of businesses called, and where a definite outcome was achieved, 55% of calls were coded as unobtainable. This means that the phone number was invalid or had disconnected, or no one on site was available to participate, or the individual was not available to participate during the fieldwork period.

Other definite call outcomes included:

- A refusal to participate (17%);
- The individual was not contactable or available due to COVID-19 (13%);
- The business had been called the maximum number of times (8%); and
- The business was in an out of scope sector or size (1%)

Among businesses that refused to participate in the survey, a 'company policy' was cited as the main reason for refusal. There were also other businesses that were not directly contactable due to COVID-19, in most of these cases, the interviewing team was able to pass on an email via the call-handler or receptionist.

To help understand why some businesses were not able to take part in the interview, codes were added to the interviewing script to help identify the underlying reasons. Data was recorded for 248 businesses who said that there was nobody on site that would be suitable to complete the survey. The main reason given was that IT and/or cyber security is either outsourced to a third party or is handled by Head Office or a branch outside of the UK (68%). Around one-quarter (27%) of these businesses gave a variety of reasons, including a 'no name / email' policy, the businesses did not have an IT department or no one had the responsibility for connected devices within the organisation and would therefore not be suited to answer the intended questions. The remaining 13% did not specify why there was no one on site that would be suitable to complete the survey. This analysis suggests that there is a sizeable proportion of businesses whose management (including usage and procurement) is dealt with externally, with the 'next best' individual in the company (e.g., IT director or manager) having little or no knowledge of how these devices are used and managed on a daily basis within the organisation.

Recruitment challenges

During the pilot fieldwork phases, it became clear that it was significantly more challenging to secure interviews than anticipated, for two primary reasons. Firstly, it was a complex process to identify and

access the most appropriate individual within the organisation and, secondly, it became apparent that it was more difficult than usual to gain their consent to participate in an interview.

After the pilot fieldwork phases, the following changes were made to the survey introduction to aid the receptionist or call-handler in progressing the interview request:

- Reduced the use of detailed and technical language in the survey introduction, for example using a brief definition of 'connected devices'
- Removed references to 'cyber security': this caused some call-handlers a degree of concern about the authenticity of the call
- Simplified the request by asking to speak to the 'Head of IT' or 'IT department', from which the request could be progressed further. This was based on the assumption that individuals under this remit would be much more likely to understand the subject matter and be able to signpost us to the right person with ease (if not them).

The changes listed above had a positive effect in helping to relay the interview request to the receptionist / call-handler; however, it did not go far enough to enable us to reach the initial target of 400 interviews overall. Table 3.4 sets out the further actions taken on sampling.

Table 3.4 Additional sample source explored and outcomes

Additional sample source explored	Outcome
Desk research	Desk research was carried out for businesses where the receptionist / call-handler advised that they could not put our call through unless we specified a named individual i.e., a 'no names' policy or where the number was incorrect. Contact names and telephone numbers were identified from business' websites and these details were updated in the sample throughout the fieldwork period.
DCMS industry signposting	DCMS passed on the survey information webpage and IFF Research team contact details to industry leads. Leads were advised to contact IFF directly should they wish to participate.
Additional sample source of IT directors	A commercial database of c. 1,500 IT professionals was procured and loaded in towards the latter part of the fieldwork period. This sample source yielded 15 interviews.

4 Use of connected devices within organisational networks

This chapter outlines how connected devices are used within organisational networks, including the range of devices within use, who is responsible for their oversight, the use of devices that cannot be monitored by the installation of third-party apps or software, and the importance of third-party digital services.

Key findings

There was a wide range of connected devices in use within organisational networks, with some large businesses using devices into the 1,000s. Most businesses, but not all, kept track of the number of devices in use within their networks. In the majority of businesses, more than one individual was typically responsible for: cyber security, IT architecture, and the procurement and management of connected devices. Around one-quarter of businesses said they used connected devices that cannot be monitored for security issues through the installation of apps or software.

Number of connected devices used within organisational networks

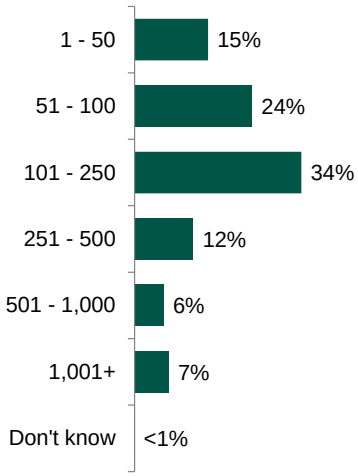
Businesses reported a wide range of connected devices used within organisational networks, ranging from 6 to 50,000 devices. Most commonly, businesses deployed between 101-250 devices within their network (34%).

Fifteen medium-sized businesses reported that they had fewer than 50 connected devices in use (ranging from 6 to 45 devices), which would mean that not all staff had access to their own commonly used business device such as a desktop or laptop computer, VoIP telephone, or a smartphone. It is likely that these participants did not consider such everyday devices in their responses and under-reported the scale of devices in use within their network.

Large businesses used a significantly greater number of connected devices, compared to medium businesses. Around one-fifth (19%) used between 501-1,000 devices, whereas only 4% of medium businesses deployed this number of devices. Over one-third (36%) of large businesses used over 1,000+ devices within their network, whereas just 1% of medium-sized businesses used connected devices at this scale.[5] This suggests that larger businesses are at a greater risk of security threats, by virtue of their significantly greater use of connected devices.

[5] Other studies, such as by Infoblox in 2020 found that a significant majority of businesses (78%) had more than 1,000 devices connected to their networks on a typical day, including 48% who had between 2,000 and 10,000 devices in use. It should be noted that this study surveyed countries other than the UK. Data for the UK only as well as business sector and size is not stated in this report, as a result this reference should be considered as indicative only.
"What's Lurking in the Shadows 2020?," 2020, https://www.infoblox.com/wp-content/uploads/infoblox-whitepaper-whats-lurking-in-the-shadows.pdf.

Figure 4.1 Number of connected devices used within organisational networks



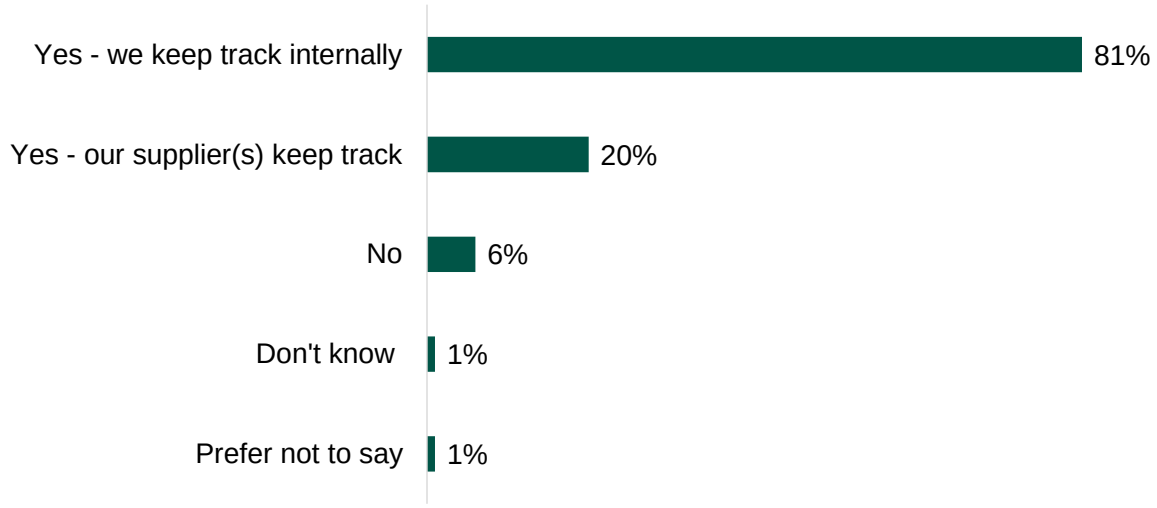
	Business size	
	Medium (50-249)	Large (250+)
1 - 50	19%	0%
51 - 100	27%	11%
101 - 250	39%	11%
251 - 500	10%	21%
501 - 1,000	4%	19% ↑
1,001+	1%	36% ↑
Don't know	0%	3%

Base: A1/A1b. In total, how many connected devices are in use within your organisation's network? All businesses (n=124)

↓↑ *Denotes statistically significant differences between sub-groups*

Most businesses (93%) said that they keep track of how many connected devices are deployed within their network, either internally (81%) and/or through their suppliers (20%). A minority of businesses (6%) said that they do not keep track of the number of connected devices deployed within their network. Businesses in the Transportation & Storage sector were significantly less likely to keep track of how many devices are in use (14%) compared to the average among all businesses (6%).

Figure 4.2 Keeping track of the number of connected devices deployed within organisational networks



B1. Does your organisation keep track of how many connected devices are deployed in your network?
Base: All businesses (n=124)

Responsibility for cyber security, IT architecture, and procurement and management of connected devices

Responsibility for cyber security, IT architecture, and the procurement and management of connected devices was typically shared by more than one individual (69%). Just under a third (30%) of businesses reported that one individual was responsible for cyber security, IT architecture, and the procurement and management of connected devices.

Businesses in the Research & Development sector were significantly more likely to share the responsibility across more than one individual (86% vs. 69% average), whereas businesses in the Transportation & Storage sector were significantly more likely to report that one person held the responsibility for all three areas (47% vs. 30% average).

Among businesses where responsibility for cyber security, IT architecture, and the procurement and management of connected devices was shared, the most common job roles within this remit were: IT Manager (40%), other IT roles e.g., consultant, supervisor or technician (34%) and other various managerial roles (20%). Similarly, for businesses that had one individual that holds responsibility, their job role was most commonly an IT Manager (33%).

Usage of connected devices that cannot be monitored

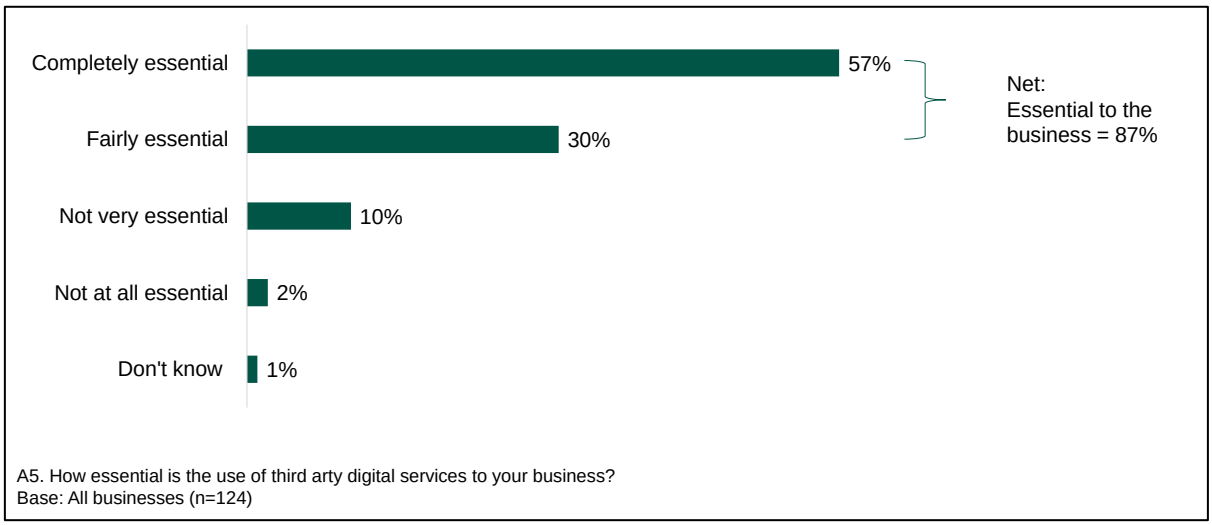
Just over one-quarter (27%) of businesses said they used connected devices that cannot be monitored for security issues through the installation of apps or software, while the majority of businesses (67%) said they did not use such devices. Commonly used devices in a business setting such as printers and VoIP phones are not compatible with security monitoring apps or software, this suggests that the use of connected devices that cannot be monitored is more widespread than this finding suggests. This highlights that many businesses may not have considered such commonly used devices in their answer, and the potential for printers and VoIP to act as security threats may be less top of mind among IT professionals.

Businesses within the Research & Development sector were significantly more likely to not use connected devices that were unable to be monitored (82% vs 67% overall). Additionally, businesses with an annual turnover of £10m+ were more likely to report they did not use connected devices that were unable to be monitored (77%).

Importance of third-party digital services

The majority of businesses (87%) felt it was essential to use third-party digital services, with only a handful of businesses (2%) reporting that these were ‘not at all essential’ to the business.

Figure 4.3 Importance of third-party to digital services to the business



A5. How essential is the use of third arty digital services to your business?
Base: All businesses (n=124)

Businesses with 101-250 connected devices were significantly more likely to report that third-party digital services were 'completely essential' to the business (73%), compared to the average of all businesses surveyed (57%) and to businesses with more than 250 devices in operation (45%).

Medium-sized businesses were significantly more likely to say that third-party digital services were 'completely essential' to their business (63%), compared to large businesses (31%).
It was typically medium-sized businesses that deployed between 101-250 devices (39% vs 11% among large-sized businesses), and indeed when taking medium-sized businesses as a whole, they were significantly more likely than large businesses to report that it was completely essential (63%) to use third party digital services (63% vs 31%).

Guidance published by NCSC[6] exemplifies the advantages and risks of adopting a range of popular Software as a Service (SaaS) applications, also known as third-party digital services. From this, it can be inferred that there are variations in the extent to which third-party digital services effectively mitigate against security threats when in use in organisational networks. As a result, this finding suggests that medium-sized businesses may be more vulnerable to security threats that use third-party digital services as a vector of attack, owing to their greater reliance on third-party digital services compared to large-sized businesses.

[6] "Product Evaluations", ncsc.gov.uk, November 19, 2018, https://www.ncsc.gov.uk/collection/saas-security/product-evaluations

5 Procurement of connected devices within organisational networks

This chapter explores how connected devices are procured, including any security checks that need to be undertaken by businesses. It also outlines the manufacturers of connected devices that are used within organisational networks.

Key findings

Around six in 10 businesses did not require any security and procurement related checks before purchasing connected devices, this was more common among medium-sized businesses. Among those who required such checks, a range of actions were required, however there was no unifying theme. Using an approved suppliers list received most mentions, followed by carrying out internal checks or testing, and background checks such as credit, legal, financial, or research.

Among businesses who said they undertake security and procurement related checks before purchasing connected devices, the most common process involved holding ad-hoc meetings to discuss any network changes, and the use of a documented communication trail.

Over one-third of businesses were unable to specify the manufacturers of connected devices in use within their networks. The most commonly mentioned manufacturer for devices (excluding servers, laptops, desktops, and smartphones) was HP, followed by Dell and Cisco.

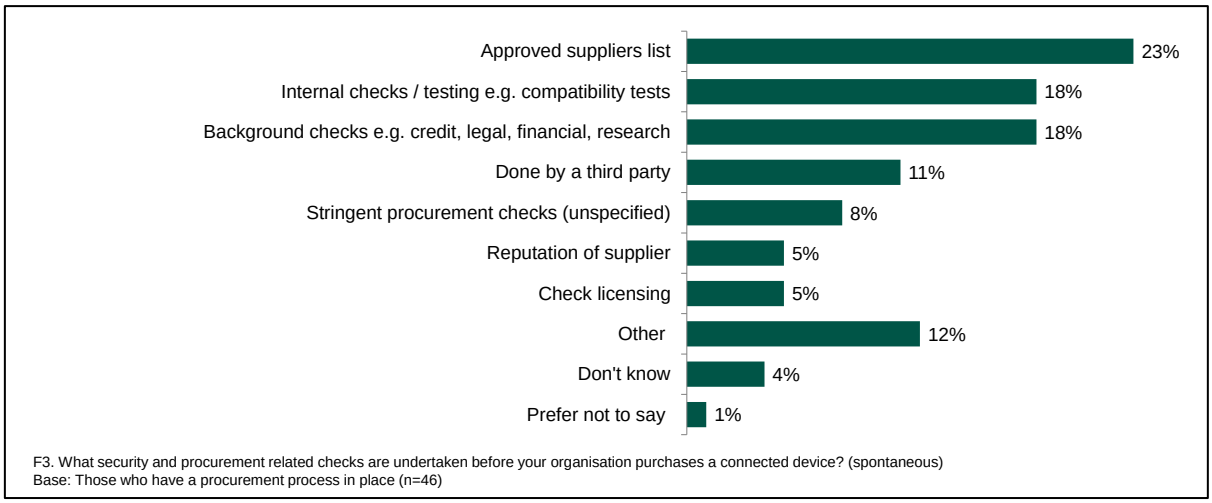
Security checks during procurement

A third (33%) of businesses said they have some form of security and procurement related checks that have to be undertaken before purchasing connected devices. Nearly six in ten (58%) said they did not, 7% said they did not know, and 1% declined to answer. Large businesses were much more likely to have such checks in place (52%) than were medium-sized businesses (29%).

Businesses in the Research & Development sector were significantly less likely than others to say they had no checks in place (41%), as compared with 58% of all businesses.

The third of businesses that did have any procurement processes in place were asked to say in their own words, what checks were undertaken before purchasing a connected device. Figure 5.1 shows that most common processes were to have an approved suppliers list (23%), to carry out internal checks (18%) or to carry out background checks such as credit, legal, financial or research (18%). There were no significant variations by business size or sector.

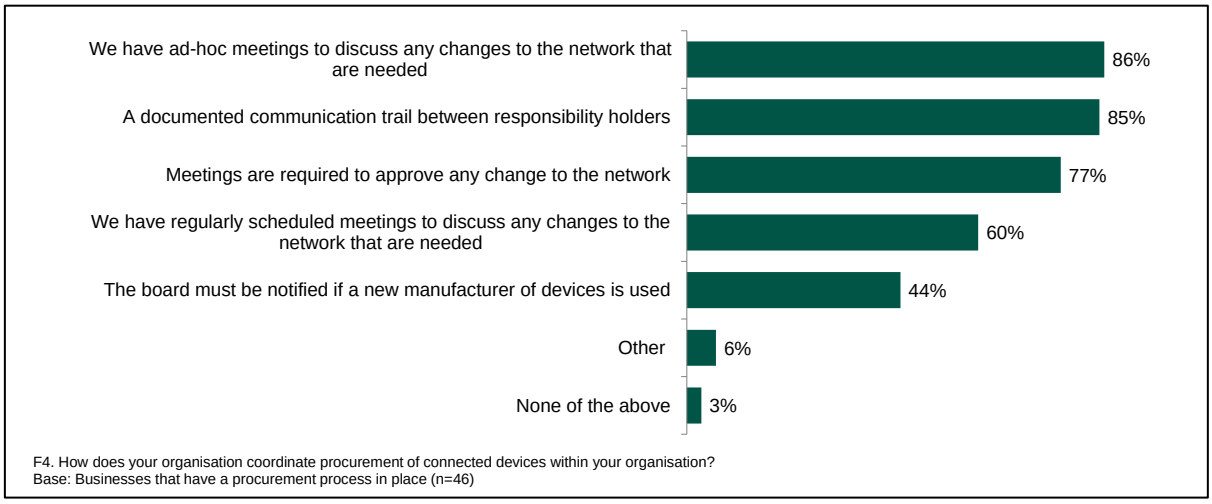
Figure 5.1 Security and procurement related checks undertaken before organisation purchases a connected device



F3. What security and procurement related checks are undertaken before your organisation purchases a connected device? (spontaneous)
Base: Those who have a procurement process in place (n=46)

Among businesses who said they undertake security and procurement related checks before purchasing connected devices, the most common requirements were to hold ad-hoc meetings to discuss any network changes (86%), provide a documented communication trail (85%), and the requirement to hold a meeting to approve any change to the network (77%). The majority of these businesses also have regularly scheduled meetings to discuss any changes to the network (60%) and to notify the board if a new manufacturer of devices is used (44%).

Figure 5.2 How businesses coordinate procurement of connected devices



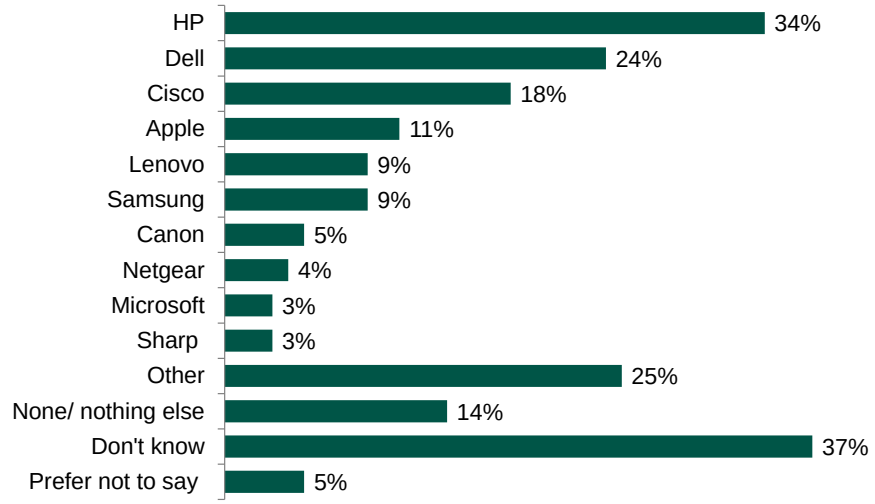
F4. How does your organisation coordinate procurement of connected devices within your organisation?
Base: Businesses that have a procurement process in place (n=46)

Manufacturers of connected devices

Excluding servers, laptops, desktops, and smartphones, businesses were asked to state the top three manufacturers that they purchase devices from where those devices are connected to their organisation's network. HP was the brand leader among both medium-sized (32%) and large businesses (40%); and across all five industry sectors. This was followed by Dell (24%) and Cisco (18%).

Over a third (37%) of respondents were unable to answer this question. Figure 5.3 lists other manufacturers that were used by at least 3% of businesses.

Figure 5.3 Top manufacturers that businesses purchase connected devices from (≥3% of mentions)



F1. Excluding servers, laptops, desktops and smartphones; please list the top three manufacturers that you purchase devices from where those devices are connected to your organisation's network? Base: All businesses (n=124). Manufacturers cited by fewer than 3% are not shown.

There were also some other manufacturers cited by 2% or 1% of businesses, namely: Kyocera, Ricoh, Mitel, Watchguard, Ubiquiti, Zebra, Toshiba, LG, OKI, SonicWall, Nokia, Siemens, Yealink, DrayTek and IBM. There were no significant variations by business size or sector.

6 Management of connected devices within organisational networks

This chapter explores how businesses manage security risks to their use of connected devices, their experience of cyber-attacks and mitigation strategies, and the types of cyber-security insurance that businesses use to manage such risks.

Key findings

Around one in five businesses did not have a formal process for managing remote access by third parties or external suppliers, and one in 10 did not have any agreements in place with suppliers of connected devices in relation to their safe and secure use.

While the majority of businesses keep track of potential threat vectors, either internally or in combination with their suppliers, around one in five businesses said that either only their suppliers keep track or that they do not keep track at all.

In the event of a cyber security attack, the top planned actions where to: hold a meeting with the key responsibility holders, engage with the Data Protection Officer, notify the ICO and establish dedicated comms channels between the responsibility holders using corporately linked IT.

Nearly half of businesses had a cyber-security insurance cover: either as part of a broader insurance policy or as a standalone policy, while around one in five said they had no such insurance. Among the businesses that had cyber-security insurance, around one in four businesses did not know whether it provides cover for cover for cyber security attacks stemming from connected devices on their networks.

Managing security risks to the use of connected devices within organisational networks

Managing remote access

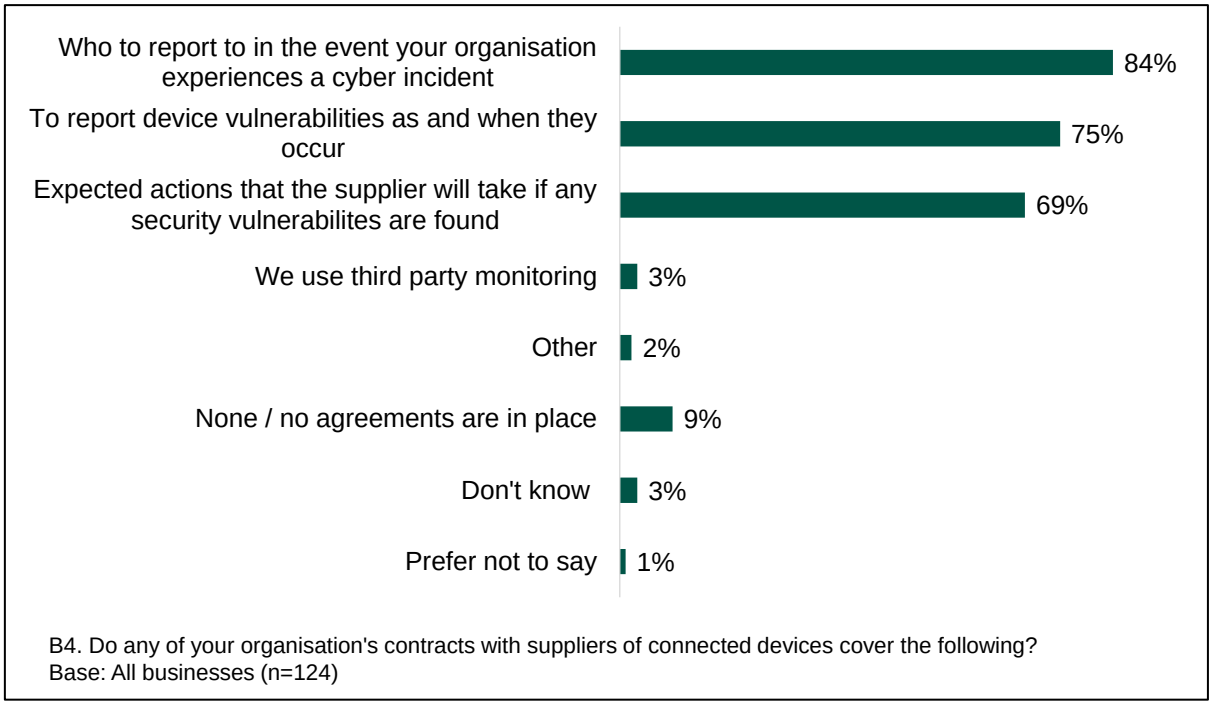
The majority of businesses (76%) had a formal process for managing remote access by third parties or external suppliers who are involved in the management and maintenance of their connected devices, while around one-fifth did not (22%).

Contracts with suppliers of connected devices

Most businesses' contracts with suppliers of connected devices covered: who to report to in the event the organisation experiences a cyber incident (84%), to report device vulnerabilities as and when they occur (75%) and the expected actions the supplier will take if any security vulnerabilities are found with connected devices (69%). A minority of businesses (3%) used third party monitoring. Around 1 in 10 (9%) businesses did not have any agreements in place with their suppliers of connected devices.

Businesses with more than 100 connected devices in use within the organisation were significantly less likely to have contracts with suppliers that covered who to report to in the event their organisation experienced a cyber incident (78%) compared to businesses who use 100 or fewer devices (93%).

Figure 6.1 What contracts cover with suppliers of connected devices



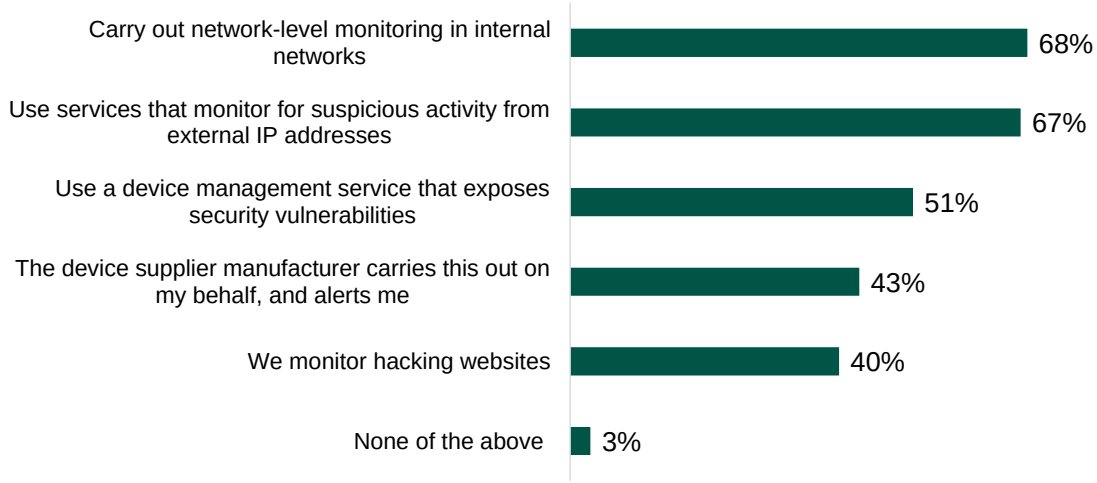
B4. Do any of your organisation's contracts with suppliers of connected devices cover the following?
Base: All businesses (n=124)

There were no significant differences seen by sector for what supplier contracts cover.

Device monitoring

Around a quarter of businesses surveyed used connected devices that could not be monitored through the installation of apps or software (27%).[7] Of these businesses, the most common methods for monitoring their devices included: carrying out network-level monitoring in internal networks (68%) and the use of services that monitor for suspicious activity from external IP addresses (67%). Other common methods reported included the use of device management services (51%), relying on device suppliers/manufacturers to carry this out on organisations' behalf (43%) and monitoring hacking websites (40%). There were no significant differences seen by size or sector.

Figure 6.2 How businesses that cannot monitor devices through apps or programmes monitor devices within their organisation



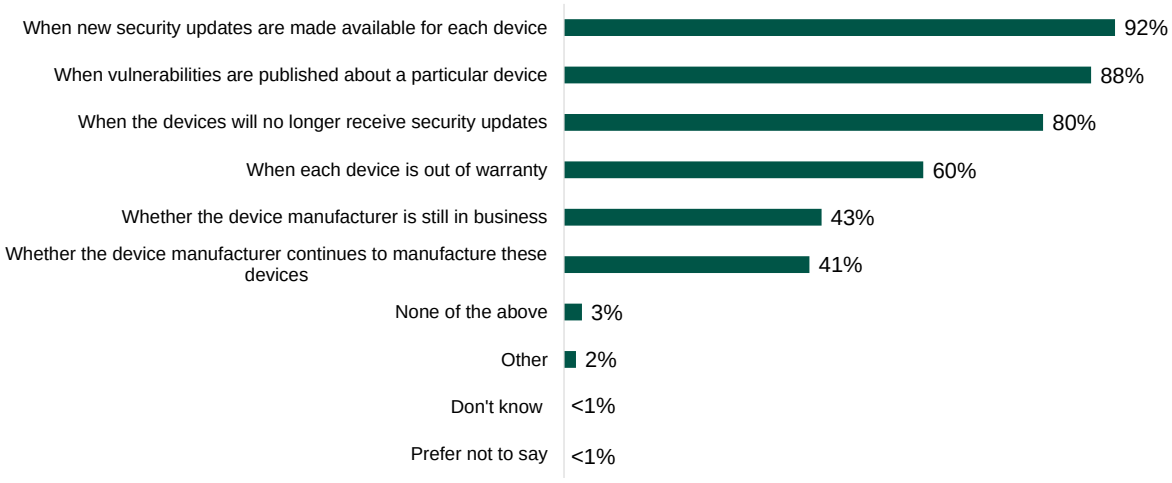
C5. How do you monitor the use of these devices within your organisation?
Base: Businesses that cannot monitor connected devices through the installation of apps or programmes (n=34).
Caution: Low base.

For businesses' connected devices, the majority of respondents most commonly monitored when new security updates are made available (92%), when vulnerability notices are published about a particular device (88%) and when the devices will no longer receive security updates (80%). Six in ten (60%) businesses monitored when each device is out of warranty [8], while just four in ten each monitored whether the device manufacturer is still in business (43%) and whether the device manufacturer continues to produce the devices in question (41%). By sector, businesses in Research & Development were significantly more likely to monitor when each device is out of warranty (78%), compared to the average of all businesses surveyed (60%).

[7] In this same vein, a global study from Gemalto found that only around half (48%) of businesses can detect if any of their IoT devices suffer a breach. Moore, B. 2019. "Half of companies unable to detect IoT device breaches", SecurityBrief, 16 January 2019. https://securitybrief.eu/story/half-of-companies-unable-to-detect-iot-device-breaches

[8] It is important to note that for many devices, a warranty does not at present disclose the length of time a device will receive security updates. Therefore when 60% say they are monitoring this, it does not necessarily mean they are monitoring security updates. Future legislation by the UK Government will require this for consumer connected products.

Figure 6.3 Monitoring of connected devices

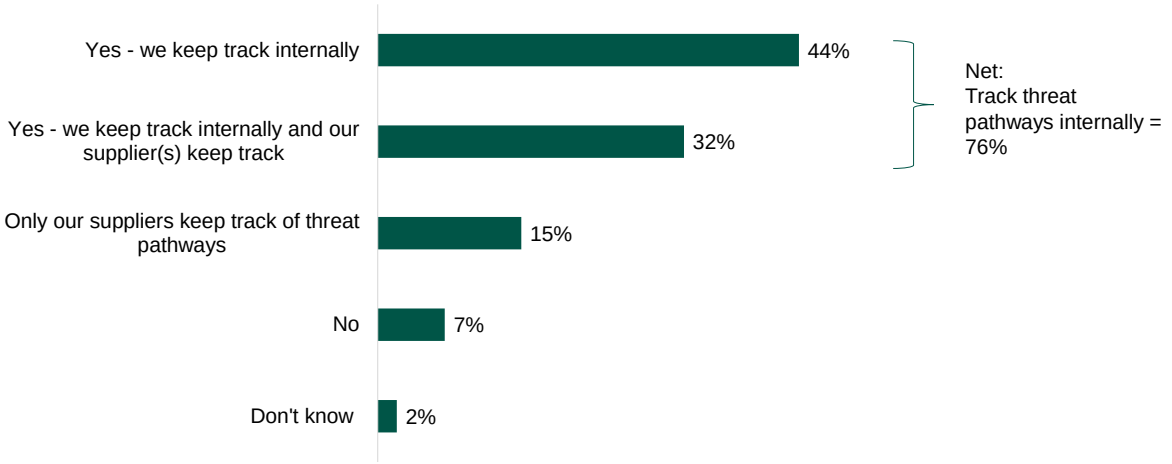


C4. Which of the following does your organisation monitor in relation to the connected devices that are in use within your organisation's network?
Base: All businesses (n=124)

Tracking potential threat vectors

The majority of businesses said they keep track of potential threat vectors for the devices that are connected to their organisations network (76%); 44% of these businesses keep track internally and 32% keep track internally alongside their suppliers. Some businesses reported that they only rely on their suppliers to keep track of potential threat vectors (15%) and a minority of businesses report they do not keep track of potential threat vectors at all (7%).

Figure 6.4 Keeping track of potential threat vectors for devices connected to organisational networks



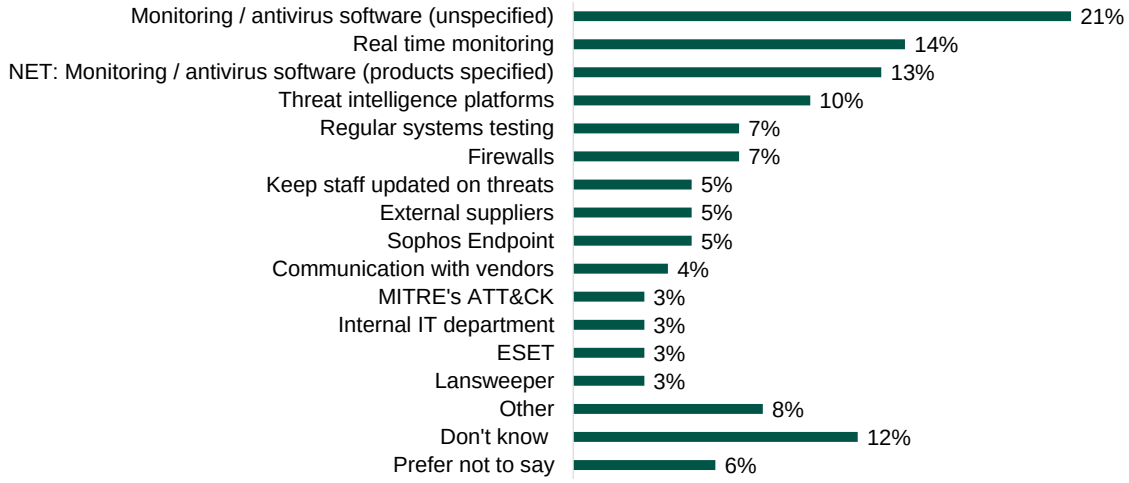
C1. Does your organisation keep track of the potential threat vectors for the devices that are connected to your organisation's network?
Base: All businesses (n=124)

Large businesses were significantly more likely to only keep track internally of potential threat vectors for the devices that are connected to their organisations network, compared to medium sized businesses (61% vs. 41%). By sector, Transportation & Storage businesses were more likely to report that they rely on their suppliers to keep track of potential threat vectors (27%), compared to the average of all businesses interviewed (15%).

Businesses with 100 or fewer devices in use were significantly more likely to only rely on their suppliers to keep track of potential threat vectors (28%), compared to businesses that deploy between 101-250 devices (9%) and those that deploy 250+ devices (2%).

Businesses who said they keep track of threat vectors were asked to state in their own words how they keep track. A range of responses were given yet there was no common approach. Around one in five (21%) said they used some form of monitoring or anti-virus software but did not mention the specific product name; just 13% provided the specific monitoring or anti-virus product name when asked to state how they track of potential threats. A further 14% said they carried out real time monitoring, and 10% used threat intelligence platforms, while 7% each used regular systems testing and firewalls. Figure 6.5 shows the range of methods than businesses said they used to keep track of threat vectors internally or in combination with their suppliers.

Figure 6.5 Ways in which businesses monitor potential threat vectors (≥3% of mentions)



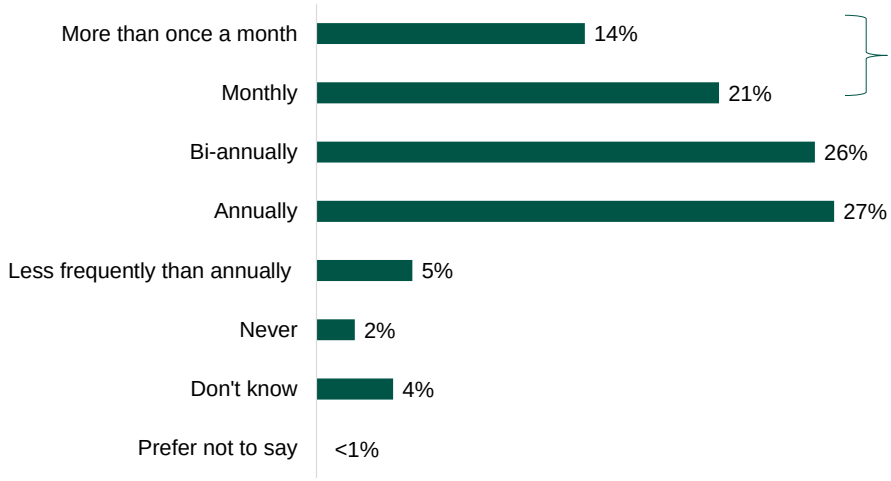
C2. How do you keep track of potential threats to the connected devices that are used within your organisation's network?
Base: Businesses that keep track of potential threat pathways (n=97)

Businesses with an annual reported turnover of £10 million or more were significantly more likely to conduct regular systems testing (14%), compared to the average of all businesses (7%), which indicates that these businesses have greater resources for internal testing.

Conducting risk assessments

Businesses were asked how often they conduct a risk assessment of the threats posed by devices connected to their organisation's network. Around one-third (35%) of businesses conducted a risk assessment at least monthly, with 14% of businesses reporting they conducted an assessment once a month. Just over one-quarter (27%) said they conduct an annual risk assessment, while 5% said they carry out an assessment less frequently than annually. Very few (2%) businesses reported that they never conduct a risk assessment.

Figure 6.6 How often businesses conduct risk assessments of potential threat pathways



C3. How often does your organisation conduct a risk assessment of the threats posed by devices connected to your organisation's network?
Base: All businesses (n=124)

Medium-sized businesses were significantly more likely to conduct a risk assessment of the threats posed to connected devices bi-annually (30%), compared to the average of all businesses (26%). By sector, Research & Development businesses were significantly more likely to conduct a risk assessment of threats more than once a month (29%), compared to the average of all businesses (14%).

Businesses with between more than 100 connected devices were significantly more likely to conduct a risk assessment less frequently than annually (8%), compared to the average among all businesses (5%).

Experience of cyber-attacks and mitigation strategies

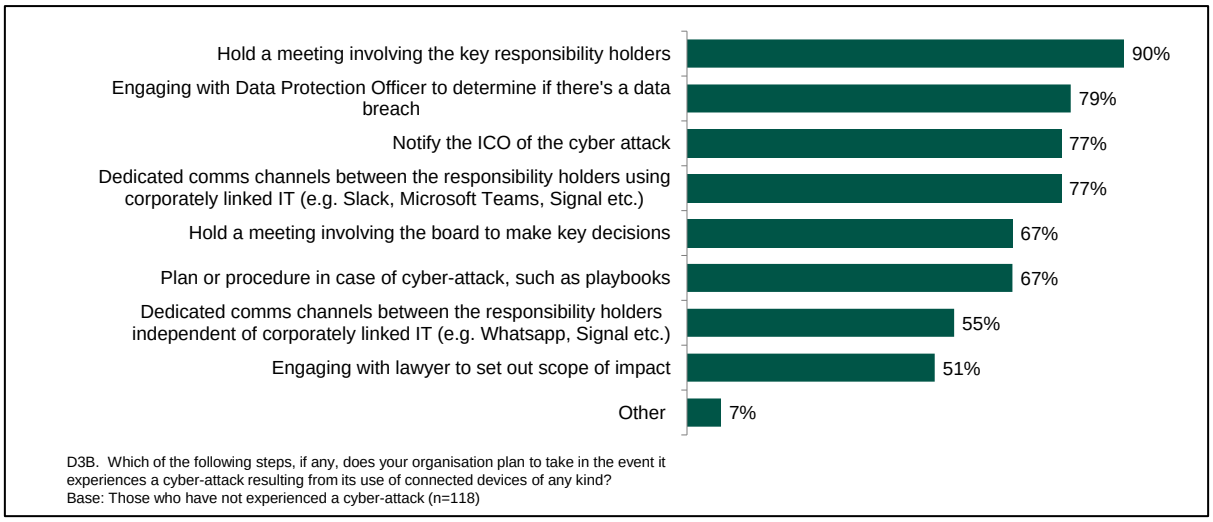
Businesses were asked whether they had experienced any cyber-attacks as a result of its use of connected devices (excluding any events occurring as a result of laptops, desktops and smartphones, as well as servers). Nearly all businesses (96%) said they had not experienced a cyber-attack of this kind, 2% each said they did not know or preferred not to answer. Only one business reported that they had experienced a cyber-attack through their use of connected devices, however they were unable to provide any detail of the attack. This finding is contrasted with the Cyber Security Breaches Survey 2021[9] (DCMS, 2021) which found that 39% of UK businesses had experienced a cyber-security breach or attack in the preceding 12 months. Although businesses were asked to exclude cyber-attacks resulting from their use of desktops, laptops, smartphones and servers from their response, it is likely that the incidence of cyber-security attacks is greater than this finding suggests. Participants may have under-reported their incidence of cyber-security attacks, either as a result of not wishing to disclose sensitive information, or a lack of awareness of such attacks having taken place through less 'top of mind' connected devices. The latter interpretation is borne out

[9] Department for Digital, Culture, Media & Sport (DCMS), 2021. Cyber Security Breaches Survey 2021 https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021
It should be noted that this research asked businesses about any cyber-security breaches or attacks experienced, and not limited to those as a result of devices other than desktops, laptops, smartphones or servers.

through findings in this research which showed that a significant proportion of businesses have infrequent and less stringent threat monitoring practices in place.

Those businesses who said they had not experienced any cyber-attacks via its connected devices were asked what steps their organisation plans to take in the event of such an attack. The top planned action was to hold a meeting with the key responsibility holders (90%). Over three quarters of businesses also said they would engage with the Data Protection Officer, notify the ICO or establish dedicated comms channels between the responsibility holders using corporately linked IT. Other specific actions were planned by between half to two thirds of businesses. The full range of planned actions is shown in Figure 6.7.

Figure 6.7 Actions businesses plan to take in the event of a cyber-attack



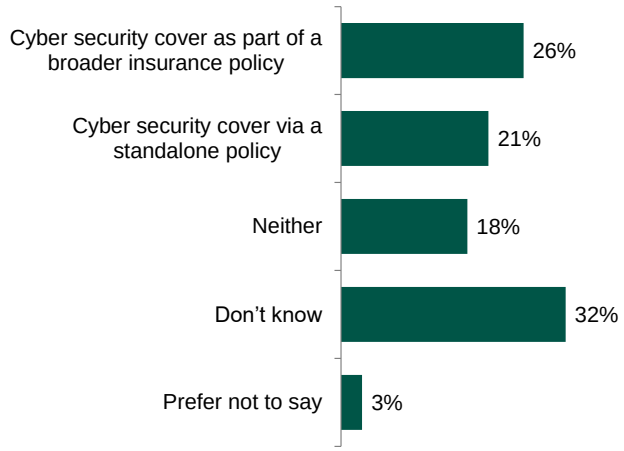
There were no significant variations in planned actions by business size or sector, apart from Transportation & Storage businesses being less likely to notify the ICO of the cyber-attack (59%) than the average among all businesses (77%).

Businesses who deployed more than 250 devices were significantly more likely to set up a dedicated comms channels between the responsibility holders using corporately linked IT compared to the average (90% vs. 77%), in addition to setting up a dedicated comms channels between the responsibility holders *independent* of corporately linked IT (70% vs. 55%).

Cyber-security insurance

Nearly half (47%) of businesses had cyber-security insurance cover: either as part of a broader insurance policy (26%) or as a standalone policy (21%). Nearly one-fifth (18%) said they had neither and a third (32%) said they did not know. A minority of 3% declined to answer.

Figure 6.8 Cyber security insurance cover



	Business size	
	Medium (50-249)	Large (250+)
Cyber security cover as part of a broader insurance policy	28%	13%
Cyber security cover via a standalone policy	23%	17%
Neither	18%	15%
Don't know	27%	55% ↑
Prefer not to say	4%	0%

E1. Does your organisation have (1) a standalone cyber security insurance policy (2) cyber security cover as part of a broader insurance policy or (3) neither?
Base: All businesses (n=124)

↓↑ *Denotes statistically significant differences between subgroups*

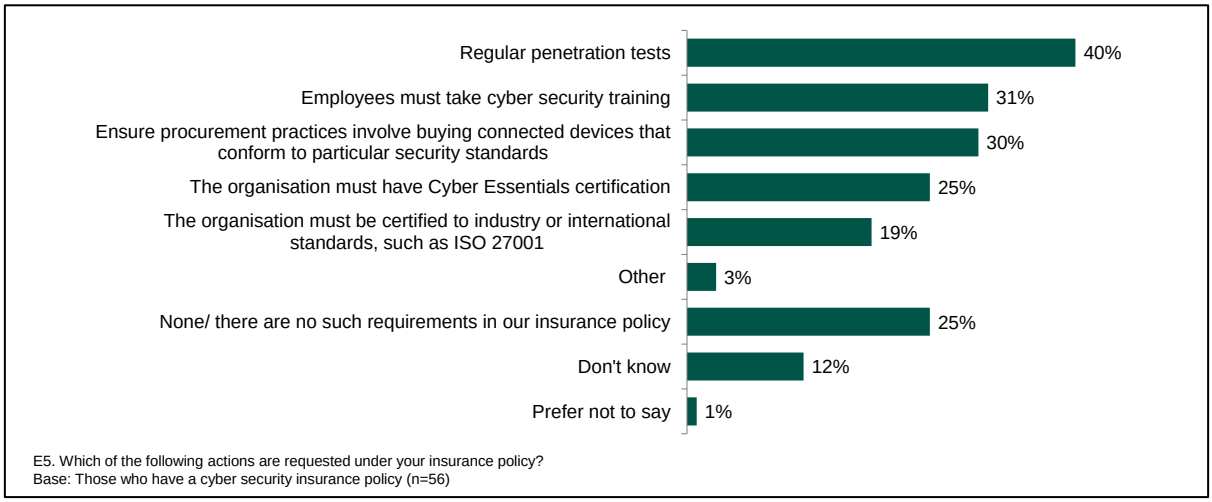
Large businesses were significantly more likely to say that they did not know whether their organisation had a cyber-security insurance policy compared to medium-sized businesses (55% vs. 27%)

By industry sector, the proportion with any cyber-security insurance cover did not vary significantly. Among the businesses that had cyber-security insurance, two thirds (68%) of them said that it provided cover for cyber security attacks stemming from connected devices on their networks, while 5% said it does not. Around one-quarter (26%) of these businesses said they did not know and 1% declined to answer. There were no significant variations by business size or sector here.

A quarter (25%) of businesses with any cyber-security insurance cover said that their insurer offered discounts on their premium as a result of taking certain specified actions (e.g., having certain processes, accreditations, or specifications in place as specified by their insurer). Around one-third (31%) said that no discounts were offered, while 42% said they did not know and 1% declined to answer. Again, there were no significant variations by business size or sector.

When asked whether any particular actions were requested under their cyber security insurance policy, a quarter (25%) said that no actions were required, and a further 12% were unsure. The remainder cited a range of different actions required, as shown in Figure 6.9: the most common requirement was for regular penetration tests (40%), followed by staff training (31%) or standardised procurement practices (30%). Again, there were no significant variations by business size or sector.

Figure 6.9 Actions requested under business' cyber-security insurance policies



E5. Which of the following actions are requested under your insurance policy?
Base: Those who have a cyber security insurance policy (n=56)

Businesses who said they have a cyber-insurance security policy were asked to provide the provider and policy names. The majority of businesses with a cyber security insurance policy did not know the provider name (55%) or were not prepared to reveal (14%). An even greater proportion of businesses (73%) did not know the name of the specific policy and 14% declined to answer. There were a few businesses who misidentified their provider name as the policy name, or vice versa.

There were a range of different policy providers mentioned by those who did cite theirs: six mentioned NFU Mutual and two mentioned each of AIG, Hiscox, and Allianz. One business mentioned each of: Aviva, CFC, CNA, Chubb, Peninsula, Red Star, Sun Alliance, QBE, OSR and Zurich; two said it was via a broker.

A few different policy names were mentioned by those who did cite theirs: two stated Cyber Edge and one business mentioned CyberClear.

“

IFF Research illuminates the world for organisations businesses and individuals helping them to make better-informed decisions.”

Our Values:

1. Being human first:

Whether employer or employee, client or collaborator, we are all humans first and foremost. Recognising this essential humanity is central to how we conduct our business, and how we lead our lives. We respect and accommodate each individual’s way of thinking, working and communicating, mindful of the fact that each has their own story and means of telling it.

2. Impartiality and independence:

IFF is a research-led organisation which believes in letting the evidence do the talking. We don’t undertake projects with a preconception of what “the answer” is, and we don’t hide from the truths that research reveals. We are independent, in the research we conduct, of political flavour or dogma. We are open-minded, imaginative and intellectually rigorous.

3. Making a difference:

At IFF, we want to make a difference to the clients we work with, and we work with clients who share our ambition for positive change. We expect all IFF staff to take personal responsibility for everything they do at work, which should always be the best they can deliver.

IFF Research

5th Floor
St. Magnus House
3 Lower Thames Street
London
EC3R 6HD
Tel: +44(0)20 7250 3035
Website: iffresearch.com