SOPHOS

Securing Growth

How cyber risks among smaller U.K. companies change with size and time

Introduction

As companies grow, they change. They introduce new business processes, technologies, head count, enter new markets, launch new products, acquire new competitors and have to comply with new or different legislation. These changes can directly impact IT security risks.

To better understand the IT security challenges facing growing companies in the U.K., Sophos, a worldwide leader in next generation cybersecurity, commissioned independent research that looked at companies by size and by how long they had been trading.

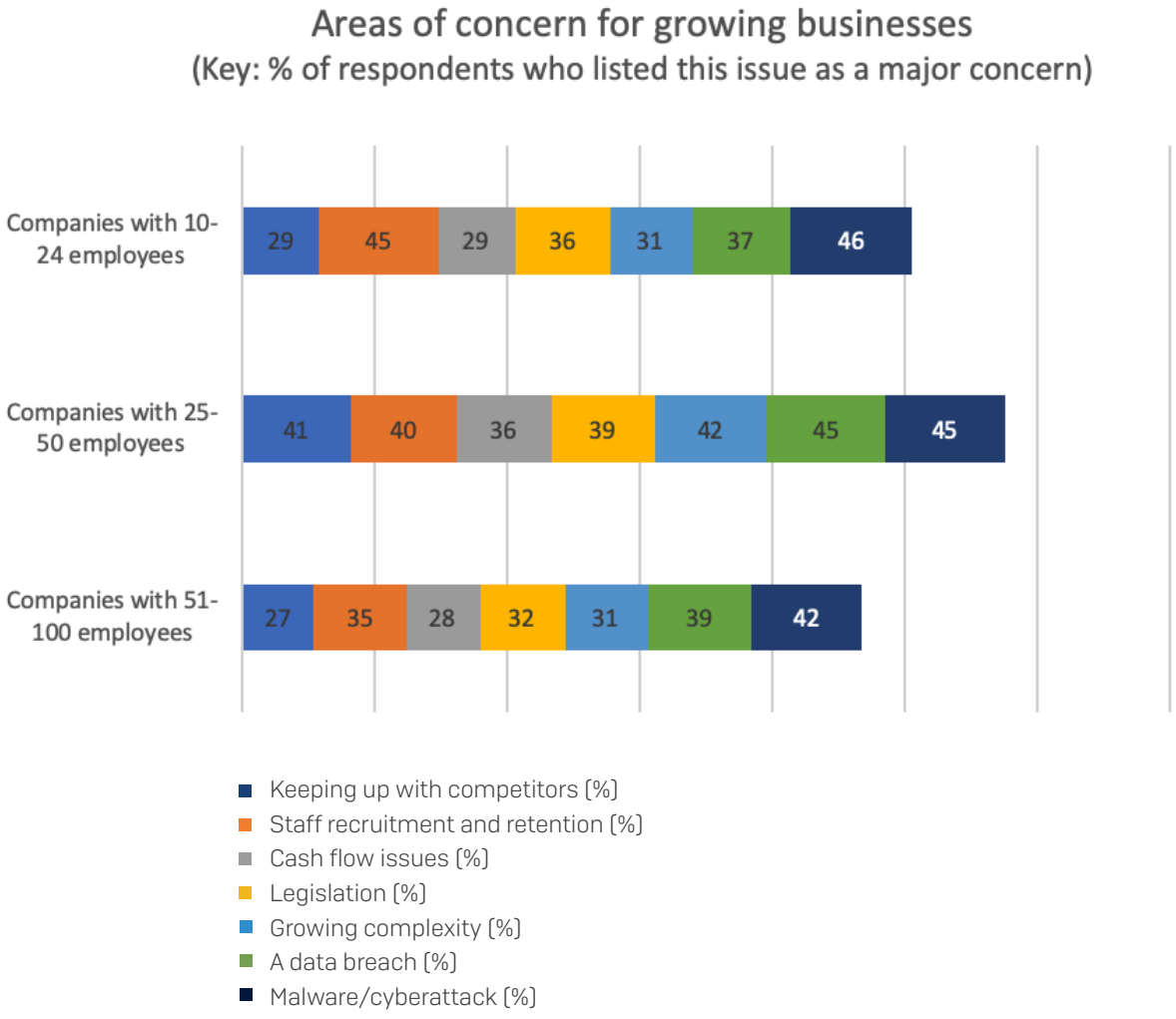
The findings challenge a few widely held assumptions: that smaller businesses aren't as concerned about cyberthreats as perhaps they should be, or that an organization's cyber risk profile can be broadly defined by its number of employees. In fact, our research suggests that the biggest risk differentiator is years of operation, and that smaller firms do worry about cyberthreats – it's just that this doesn't always translate into secure behaviour.

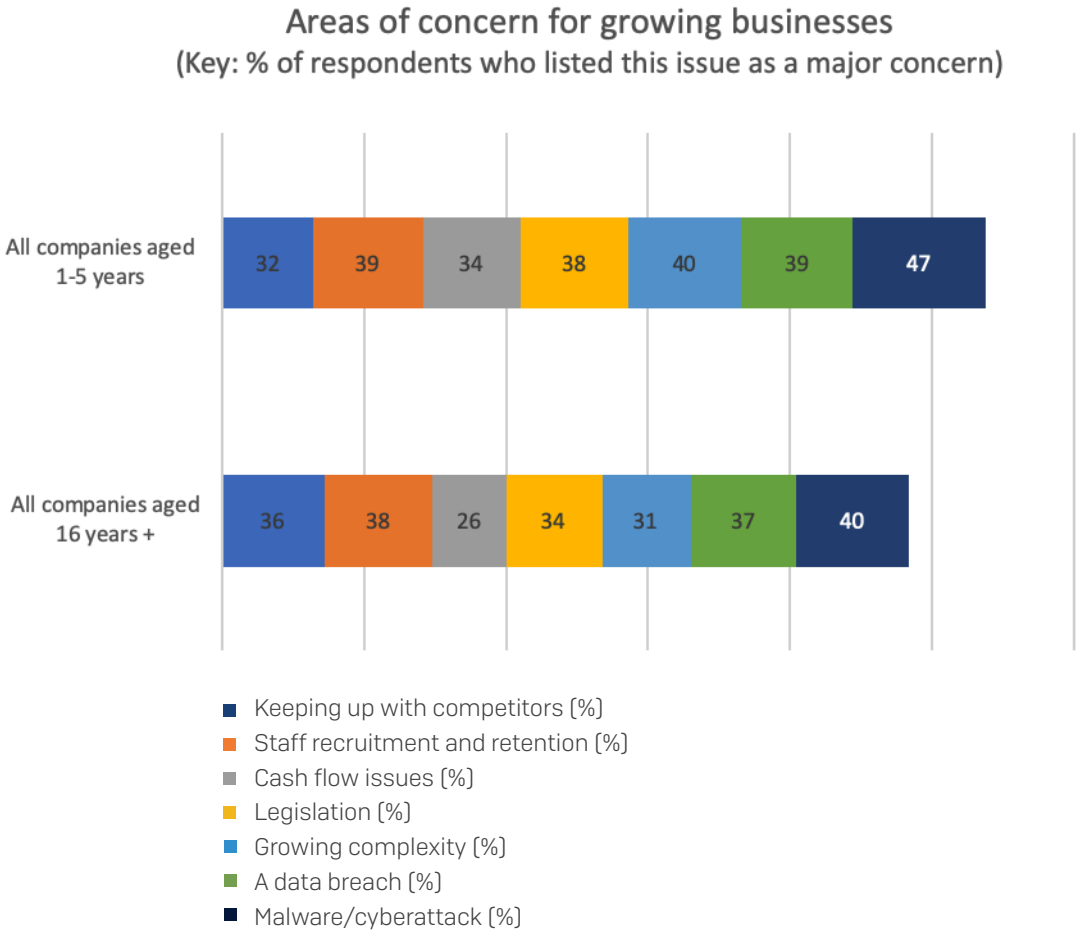
The research was conducted in late October 2019 and involved over 400 business and technology decision makers in companies with between 10 and 100 employees, trading for more than one year. The interviews were conducted online by Sapio Research.

1: What's keeping leaders of growing companies awake at night?

The short answer is everything, but particularly cyberthreats and their impact.

Almost half (45%) of all the companies surveyed say that malware infections and cyberattacks are major business concerns, followed by data breaches (42%) and then staffing issues (40%), keeping up with legislation (37%), and cash flow problems (32%).





The concern about cyberthreats may be driven in part by the widespread introduction of new technologies as companies move towards digital transformation.

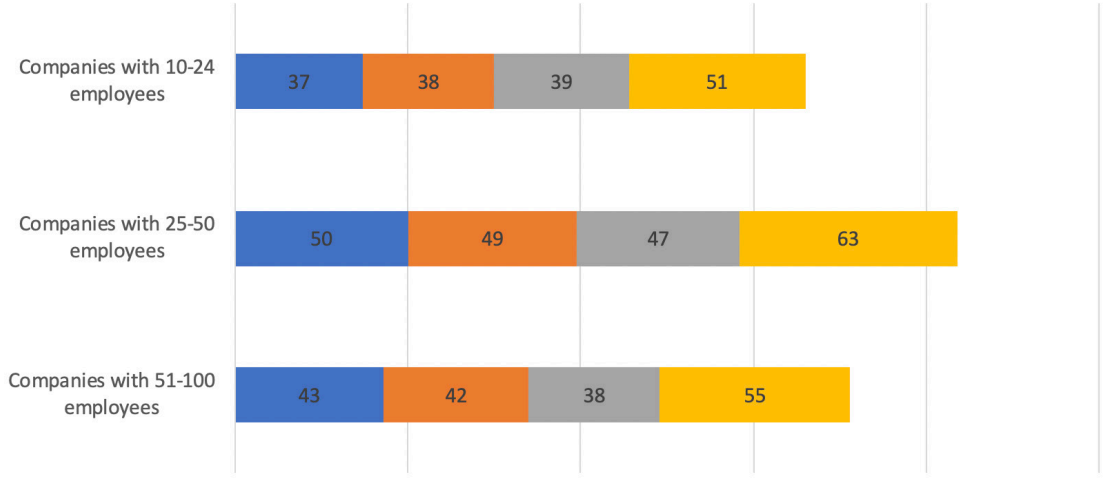
2: Digital transformation and the growing business

Around three quarters of the companies surveyed say they have introduced cloud-based services and new IT equipment into the business.

In the last year alone, around half (45%) brought in new cloud software applications to help with communication and collaboration, HR, sales, stock control, finance management, and more. Similar proportions implemented cloud data backup and storage systems (44%), new IT infrastructure, like routers and servers (43%), and new, company-owned computers, laptops, and smartphones (58%).

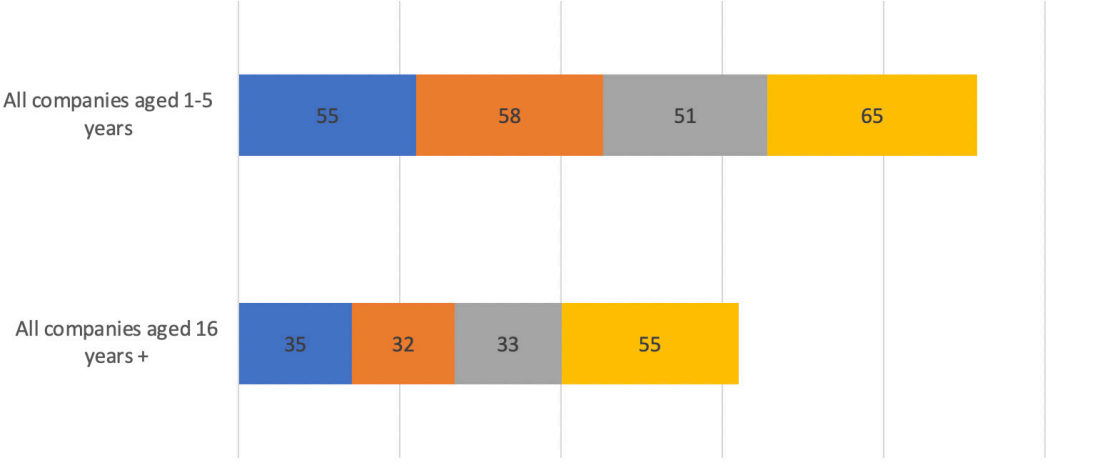
These results are fairly consistent across all the company sizes and age groups surveyed, with the exception of the longest trading businesses. Older companies are slightly more likely to have acquired what they needed over a year ago, but, overall, they lag behind other businesses with only around two-thirds introducing digital technologies at all. The only area where they match the others is in the introduction of company-owned computers and other devices.

Digital measures introduced within last 12 months – by company size
(Key: % of respondents who had introduced)



- Cloud software applications to help with any of the following: communication/collaboration, HR, sales, stock control, finance management (%)
- Cloud data backup and storage (%)
- New IT infrastructure, for example routers and servers (%)
- New company-owned computers, laptops, and smartphones (%)

Digital measures introduced within last 12 months – by company age
(Key: % of respondents who had introduced)



- Cloud software applications to help with any of the following: communication/collaboration, HR, sales, stock control, finance management (%)
- Cloud data backup and storage (%)
- New IT infrastructure, for example routers and servers (%)
- New company-owned computers, laptops, and smartphones (%)

The connected business ecosystem

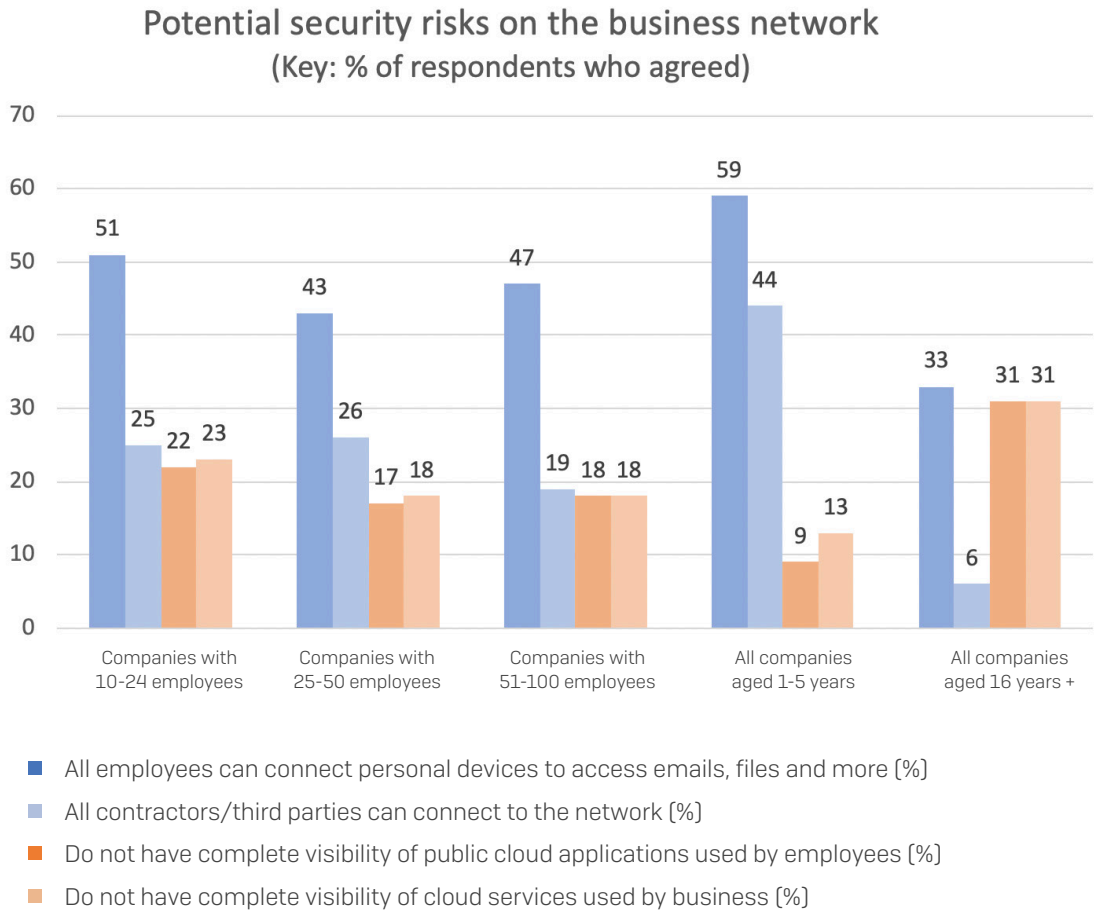
The introduction of digital technologies and cloud services helps companies to compete in an increasingly connected ecosystem, but they can also introduce new security vulnerabilities because organizations don't always have visibility into or manage what is actually happening.

Open all hours

For example, in around half of all the companies surveyed – falling to a third for companies that have been trading for more than 16 years – all employees are able to connect personally-owned devices like smartphones to the corporate network and to access work emails, documents, and more.

This approach, known as BYOD (Bring Your Own Device) can reduce IT costs and increase productivity for businesses, but it can represent a significant risk if security measures such as multifactor authentication, VPNs, etc. are not implemented and enforced by the employer.

If such precautions are not in place, the use of personal devices can offer hackers unguarded entry points they can use to breach the corporate network, escalate privileges, and move laterally to high value servers and endpoints.



Similarly, many of the companies surveyed have an open-access network policy for third parties such as contractors. This ranges from 44% for the youngest companies to just 6% for the longest running.

Limited visibility

The study also shows that more than a quarter (27%) of respondents overall are not fully aware of the specific cloud services used by their company, and 25% do not know which public file sharing applications employees are using to share information externally.

3: IT security staffing and technologies

IT support

It is encouraging that even the smallest businesses look to professional support to help them with the implementation and management of IT.

Who looks after your IT?

1. In-house IT specialist: 37% overall
2. An external IT contractor or managed service provider (MSP): 35% overall, rising to 44% for companies less than six years old
3. A combination of in-house staff and external IT contractor: 24% overall
4. Neither, IT decisions are made by non-IT specialists: 10% of companies with fewer than 25 employees

However, the survey also found that 22% of the organizations that use a contractor for IT and security support don't routinely inform them when new services, such as cloud applications, or devices are introduced, rising to 38% among the smallest firms. This means that companies could find themselves under-protected as the people implementing their security don't know there are new things to secure.

Security software

The good news is that almost three-quarters (73%) overall have installed business-grade security software, with 39% having done so in the last 12 months. However, 62% have also introduced consumer-grade security software, rising to 73% among the youngest firms, despite the fact that such products are not designed to meet the security needs of organizations. The reasons for introducing consumer grade protection, other than possibly cost, are unclear.

Businesses that have been in operation for over 16 years appear to have a better understanding of the limitations of consumer-grade protection when applied to a business environment, with 29% saying they have no plans to introduce such products. The potential benefits of such an approach are, however, offset by the fact that one in 10 (11%) of the older firms surveyed say they have no plans to introduce any business grade security software either.

4: IT security policies and behaviour

Who is in charge of protection?

It is encouraging that even the smallest businesses look to professional support to help them with the implementation and management of IT.

As might be expected among smaller businesses, senior management is fairly hands-on when it comes to defining company policies, and IT security is no exception. Over half (59%) of those surveyed say that senior managers define IT security practices such as password policies and data/network access rights and monitor whether employees are implementing security best practice (51%).

Control for implementing security practices rests largely in the hands of the IT internal and external security specialists. Software updates are managed by internal IT specialists in 44% and by external providers in 32% of businesses overall, although a third (36%) also relies on senior managers for this.

One in five of the companies with fewer than 25 'or' more than 100 employees also relies on individual employees to install updates and to self-police their own security behaviour. This drops to one in 10 (11%) among companies with 25 to 50 employees. This can create risk if employees lack cyberthreat awareness, fail to spot an update or simply forget to install it.

Employee risk awareness

Fortunately, many of the organizations surveyed claim to run cybersecurity awareness training for employees. The survey found that 74% had introduced such training, with around half (47%) doing so within the last year. However, a worrying 13% of the oldest organizations say they have no plans to introduce such training.

Supply chain cybersecurity

The findings suggest a mixed approach to supply chain security. Smaller companies can be seen by cybercriminals as a point of weakness in the supply chain that allows them to reach a larger or better protected target. As a result, many companies are seeking to shore up their supply chains by introducing security requirements for suppliers.

Eight in 10 (82%) of the companies surveyed claim to conform to cybersecurity requirements set out by customers – and 43% say they have introduced security standards for their own suppliers that have access to their data, including commercially sensitive information about the business.

However, a quarter (26%) of companies that have been in operation for 16 years or more say they have never been asked to meet any security standards, and one in 10 says they make no such demands of their own suppliers.

5: Young guns vs. old guard

One of the main threads to emerge from the research was the clear difference between companies of different ages.

Younger companies, those which have been in operation for five years or fewer appear digitally inclusive and connected, happy to seek external support, and more aware of security. However, there are significant potential risks associated with opening up their networks to third parties and employees' personal devices, and the use of consumer security products.

Older companies, established for 16 years or more, are far more restrictive about access. This gives them a security advantage, which is then offset by lower visibility in terms of cloud applications used, less emphasis on employee awareness training, and lower supply chain security.

The key message is that companies of different ages have markedly different areas of security vulnerability, and it is important that these variations are understood and addressed.

6: Cybersecurity essentials

The following check list is a guide for IT security professionals and contractors implementing security best practice in growing companies. To be effective, they should be accompanied by an ongoing program of employee security awareness training and support.

- Check that you have a full inventory of all devices connected to your network and that any security software you use on them is up to date
- Always install the latest security updates, as soon as they are released, on all the devices and servers on your network
- Have different levels of data access rights for different employees
- Keep regular backups of your most important and current data on an offline storage device as this is the best way to avoid having to pay a ransom when affected by ransomware
- Administrators should enable multi-factor authentication on any security dashboards or control panels used internally, to prevent attackers disabling security products during an attack
- Remember, there is no single silver bullet for security, and a layered, defence-in-depth security model is essential

7: How Sophos can help

Sophos has proven expertise in helping a wide range of companies of all sizes keep employees, customers, devices, and networks secure in an increasingly complex and rapidly evolving cyber threat landscape.

Alongside this, Sophos is a leader in next-generation security, offering integrated, multi-layered security solutions that are as advanced as they are easy to manage and implement, and which can adapt and grow around the ever-changing needs of an organization.

For example, Sophos Intercept X employs a comprehensive defence-in-depth approach to endpoint protection, combining multiple leading next-gen techniques to deliver malware detection, exploit protection and built-in endpoint detection and response (EDR).

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

20-01-21 SME REPORT-EN (MP)

SOPHOS