State of Technology at UK SMEs

2020 research report

OGL Computer

Table of Contents

Foreword

We are in the midst of the 4th industrial revolution, and technology is evolving faster than ever. Understanding the key trends within the technology sector will enable SMEs to prepare for, and grasp, opportunities to grow and defend their businesses.

At OGL Computer and our specialist CyberGuard Technologies division, we are proud to work with SMEs across multiple industry sectors. We surveyed IT decision-makers at just over 400 UK SMEs about the current state of cyber security and technology adoption in their companies, the challenges they face, and how they are accommodating emerging technologies and digital transformation initiatives.

The results of this intensive research are before you - the inaugural State of Technology at UK SMEs 2020 report. It reveals that the majority of IT decision-makers at SMEs have clear strategies for the future, as well as a detailed grasp of the opportunities and challenges that face their verticals in 2020.

These range from the perennial, such as the ever-present threat of serious cyber-attack or data breach, as well as effectively managing the increasing amount of data flowing through all organisations. In addition, moving to the cloud securely and an ongoing lack of technology-savvy workers emerged as key themes.

Handling these challenges, all with a fraction of the resources of their larger, corporate counterparts, requires flexibility and provides resilience that gives SMEs the power to succeed. As we head into a new decade where the only constant is likely to be change, it is heartening to learn through our survey that SMEs continue to adopt innovative products and services.

Whatever the year and decade ahead bring, I hope that our new State of Technology at UK SMEs 2020 report will be a useful tool for helping your business find the right route to power its growth.

Paul Colwell

Technical Director, OGL Computer and CyberGuard Technologies

Paul Colwell

Technical Director, OGL Computer and CyberGuard Technologies

OGL Computer

Nearly 1 in 5 (17%) IT decision-makers surveyed have no cyber strategy in place.

4 out of 5 (81%) said their fear of a cyber-attack / data breach has increased

94%

of respondents are seeing a growth in the number of remote workers they are employing and are turning to technology to support this.

94%

of IT managers surveyed agree that they are nervous about moving from an on-premise IT infrastructure to a cloud infrastructure due to fears of data security.

Research highlights

Top three key business priorities for 2020:

1. Increasing cyber security provision 39%
2. Moving towards a more proactive IT strategy 39%
3. Increasing use of data and insights 37%

The biggest technology concerns for 2020:

1. Cyber security attack 67%
2. Data management 56%
3. Lack of technology-savvy workers 54%

81% of SMEs in the UK confirmed that they had suffered a data breach or cyber-attack

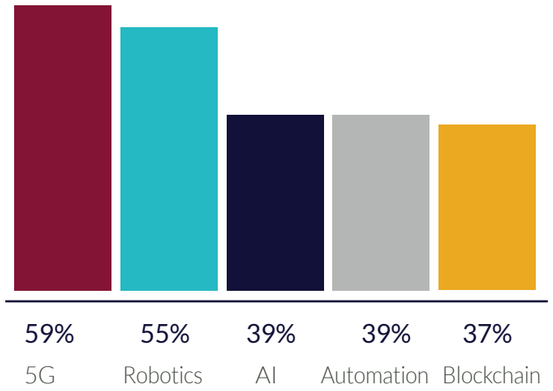
Industry sectors suffering 2 or more breaches:

- Healthcare 75%
- IT & Telecoms 75%
- Legal 66%

Industry sectors suffering 3-4 cyber-attacks:

- Finance 50%
- Manufacturing & Utilities 42%
- HR & Recruitment 37%

Emerging technologies that SMEs plan to adopt:



Technologies planned to drive business efficiencies and profitability:

- Increasing the use of applications such as Microsoft Office 365, Teams, SharePoint etc 59%
- Increasing the adoption of cloud computing 57%
- Investing in effective backup and disaster recovery solutions to ensure business continuity 55%

Reasons for new technology adoption:

- Cyber security threats 51%
- Keeping up with competitors 45%
- Attracting and retaining new talent 41%

405 IT decision-makers surveyed in England and Wales from companies with 50 – 500 employees.

98%

of companies make provision to ensure that employees are educated on how to identify a cyber threat.

92%

are planning to increase their spend on IT / cyber security.

OGL Computer

Key technology priorities

A central plank of the OGL Computer State of Technology at UK SMEs 2020 survey is to establish the technology direction SMEs are looking toward in 2020.

Top three key business priorities for 2020:

1. Increasing cyber security provision **39%**
2. Moving towards a more proactive IT strategy **39%**
3. Increasing use of data and insights **37%**

The top priorities for UK SMEs are to actively mitigate business risk, followed by increasing visibility of internal data and using that insight to gain competitive advantage.

Almost double the number of respondents in larger SME firms with 250 - 500 employees said that increasing cyber security provision was a priority compared to enabling more flexible working while maintaining security (43% vs 23%).

Increasing the use of AI and investing in digital transformation solutions were equally as important for companies with 250-500 employees

44%

Increasing cyber security provision was a key priority for businesses:

- in the healthcare sector (75%)
- with 250 - 500 employees (42%)
- with an average annual turnover of up to £10 million (61%)

Groups that favoured moving towards a more proactive rather than reactive IT strategy were respondents:

- working in the financial sector (53%)
- in companies with 100-249 employees (42%)
- working in companies with an average annual turnover of £10 - £49.99 million (41%)

Increasing the use of data and insights was the number one technology priority for respondents:

- working in companies with an average annual turnover of £50-£99.99 million (46%)
- with 50-99 employees (44%)
- in the legal (73%) and HR & Recruitment (67%) sectors

Biggest technology concerns

Looking at the other side of the technology coin, the question of concerns presented by SMEs' existing technology stacks threw up some interesting insights.

Around one in six (16%) see the risk of a cyber security attack as a greater technology concern than keeping pace with competitors, a situation clearly fuelling the skills shortage highlighted in third place. SMEs are right to be concerned about the consequences of cyber-attacks, with a recent Hiscox survey revealing that cyber breaches cost the average small business £25,700 in basic 'clear up' costs every year[1].

Despite hogging much of the news agenda in 2019, Brexit is a relatively low technology concern for 2020 – a third more respondents see a cyber-attack as more of a concern than the impact of Brexit (39% vs 67%).

Interestingly, taking these results and comparing them with the strategic priorities reveals that although two-thirds (67%) of SMEs are concerned about cyber-attacks, four out of ten (39%) plan to invest in better security provision – leaving a hardcore of three in ten (28%) who plan to take no practical action over their cyber fears.

[1] https://www.hiscoxgroup.com/news/pressreleases/2018/18-10-18

The biggest technology concerns for 2020 in business are:

1. Cyber security attack **67%**
2. Data management **56%**
3. Lack of technology-savvy workers **54%**

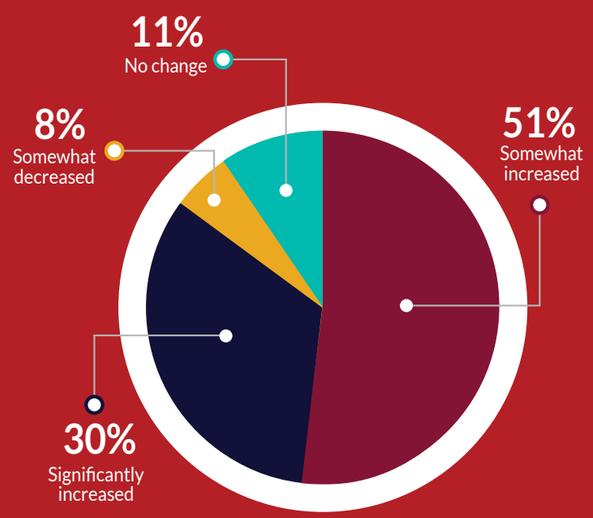
> "Businesses are waking up to cyber threats, but the lack of resource to understand and manage the technology required to mitigate attacks in-house is a major stumbling block."

Mark Slater, Senior Security Analyst, CyberGuard Technologies

Increased fear of a cyber-attack / data breach

Quantifying the level of concern around falling victim to a cyber-attack or data breach, the vast majority of SMEs confirmed that they were increasingly worried, with 81% more fearful of a cyber-attack or data breach. A mere 11% felt that there had been no change in the level of concern, while a small group (8%) had in fact decreased levels of worry.

The increased fears of falling victim to a cyber-attack or data breach could be due to many factors, including raised awareness of large-scale cyber-attacks covered by media outlets, as well as the ongoing proliferation of threats. A lack of experience and resources to track new attack vectors and vulnerabilities, as well as how to defend against them, is also likely to be a contributing factor.



"As businesses embrace new digital ways of working, many are unaware of the new security risks to which they may be exposed. Businesses need access to cyber detection tools to gain a daily view of their security posture, supported with statistics on the latest cyber threats."

Colin Dennis, Head of Technical Operations, OGL Computer

Cyber security strategy

It's hard to argue that there is a more important defence against cyber-attacks and better method of mitigating their worst effects than an actionable cyber security strategy.

The survey found that most SMEs agreed, with 83% of respondents having a cyber security strategy already in place. However, this raises the prospect that a significant number – almost one in five (17%) - of SMEs do not have a cyber security strategy in place at the moment.

"Every business should have a cyber security strategy, but an effective one requires businesses to really consider what data they hold, where they hold it, and what are the major threats they face. There are many methods that can be used to arrive at a sensible and realistic strategy that doesn't cost the earth and can also deliver real business benefits in the process."

Paul Colwell, Technical Director, CyberGuard Technologies & OGL Computer

Not only can a comprehensive cyber security strategy significantly limit the likelihood of data breaches from occurring at all, but it will also stop a smaller incident snowballing into a serious breach. This might be due to well-crafted internal security policies hindering an attacker from exfiltrating data, through to having a damage limitation strategy and notification 'call-tree' in the event of an incident being discovered. This last point – especially if customer data relevant to GDPR is involved – might prevent a sizeable fine as well as limit reputational damage.

This is why having a cyber security strategy in place is critical and considerations when developing this strategy include:

- **Be prepared**: being prepared for when, not if, the inevitable happens is key to recovery. SMEs that view cyber security as an essential foundation, with documented policies and processes, will be better positioned to withstand the after-effects of a cyber security incident.

  For instance, nearly everyone has heard of EU General Data Protection Regulation (GDPR) and understands that a breach could be very costly. By taking a proactive stance towards data protection, SMEs can take control of their data and engage with customers and prospects on a deeper and more personalised level, maximising on the opportunity to differentiate themselves from the pack.

- **Right-sized technology**: developing and implementing a cyber security strategy need not be complex or prohibitively expensive. SMEs need to seek solutions matching their size and needs which may not necessarily be the same solutions used by a larger organisation.

- **Prove security credentials**: many larger organisations often rely on a vast network of agile SME suppliers and partners. With so many data breaches occurring due to flaws in third-party partners, SMEs are coming under increasing pressure to prove their security credentials – or risk missing out on lucrative business opportunities. This is where accreditations such as Cyber Essentials Plus can prove due diligence.

Employees and cyber threats

An increasingly potent cyber-risk for businesses of all sizes is phishing, and more specifically, the business email compromise (BEC). This last threat involves an attacker taking over or entirely spoofing a key business email account – such as the MD – then changing bank account details on an otherwise legitimate invoice to those of the scammers. The main defence against this threat is good employee education, which the survey found was endemic, with 98% of IT decision-makers in SMEs educating employees about how to identify a cyber threat.

Drilling down further, the most popular approach towards employee training is using external and internal provision at 32%, while external or internal training supported by literature and information available online followed with 22% and 20% respectively. Positively, most SMEs do not feel confident enough to rely on leaflets / web links, with only 5% taking this approach.

Staff training methods to identify cyber threats:

- Internal and external **32%**
- External and leaflets / web links **22%**
- Internal and leaflets / web links **20%**
- Internal training **10%**
- External training **9%**
- Leaflets / web links **5%**
- External & internal training as well as leaflets / web links **1%**

Those bucking the trend and stating that they are more likely to provide internal training are respondents:

- working in larger SMEs with 250-500 employees 75%
- based in Greater London 72%
- working in companies with an average annual turnover of £10-£49.99 million 76%

In a recent survey of 251 IT managers in SMEs[2], CyberGuard Technologies revealed that a worrying number of UK businesses still aren't aware of the benefits of the Cyber Essentials scheme, which is supported by the National Cyber Security Centre (NCSC). Almost 1 in 5 IT managers reported that they were unaware of how compliance with the government-backed scheme could help their business, with 10% unsure of whether their company even had the certificate.

What is Cyber Essentials?

Cyber Essentials is a government-backed accreditation that was introduced back in 2014, and offers businesses baseline cyber security provision. This scheme was introduced to make it easier for businesses to protect themselves and to encourage good cyber security practices.

Cyber Essentials also offers organisations the opportunity to highlight their commitment to working securely so their customers can continue working with them, confident in the knowledge they are taking cyber security seriously and taking a proactive stance towards it.

The UK Government believes that being Cyber Essentials accredited could prevent "around 80% of cyber-attacks" and is crucial in improving your cyber security.

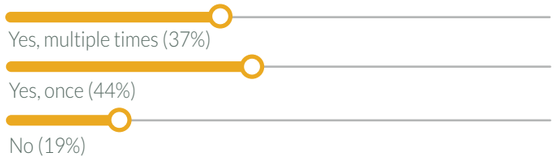
[2] https://www.ogl.co.uk/benefits-of-cyber-essentials-accreditation

Number and frequency of cyber security breaches

If any further data were needed to underscore the seriousness of the cyber-security challenge faced by businesses, then this area of the survey certainly delivered. The vast majority of UK SMEs (81%) confirmed that they had suffered a data breach or cyber-attack, with a considerable two in five (37%) admitting they had suffered multiple breaches.

Industry verticals had a significant bearing here, with the healthcare, IT & telecoms and legal industries topping the list of those suffering multiple attacks.

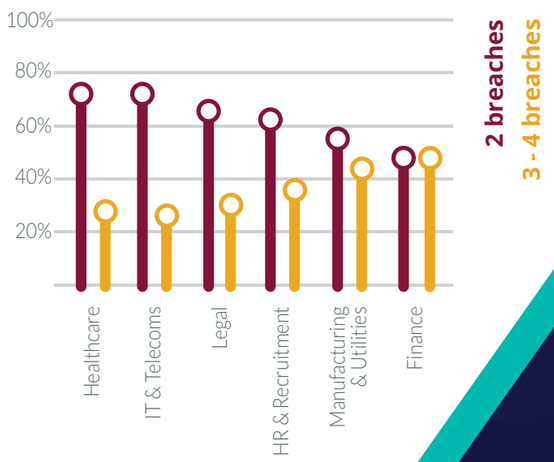
When asked if an SME had suffered an attack, SMEs said:



One respondent admitted that their company had suffered 8 or more attacks.

Of those respondents who had suffered a breach more than once, SMEs said:

Industries most vulnerable to cyber-attacks having had more than one breach:



"As an SME, it makes sense to outsource security and incident response services to a specialist cyber security provider rather than maintain in-house resources or rely on your IT support provider. However, as a business, you can't outsource your accountability to your customers for due diligence. There is still a need to train internal teams to recognise a cyber security incident."

Emma Porter, Head of Legal & HR, OGL Computer

Reasons to attack key industries

Healthcare

Public sector healthcare providers are particularly susceptible to supply chain attacks that exploit the chain of trust, targeting the valuable personal data which healthcare providers store and process. Suppliers can be seen as more vulnerable and an easier route for attackers to gain access to a more lucrative target. Hospitals store an incredible amount of valuable, confidential patient data which hackers can sell on easily – making any supplier to the industry a target.

IT & Telecoms

Some IT companies may store large amounts of sensitive customer data, while cloud storage and computing service providers, developers of security software, or file-sharing solution providers, are often the targets of supply chain compromise attempts.

Direct attacks seek to access the organisation's network operations and data while indirect attacks target subscribers within the telecoms sector. SME suppliers may be a gateway into the network - once inside, cyber criminals can easily access data and intercept calls, as well as control and impersonate subscribers.

Legal

The legal sector is particularly vulnerable to cyber-attacks due to the volume of data, sensitive information, financial responsibility and authority held. If a law firm specialises in corporate or property law, they are at increased risk, as the potential for financial gain is greater. Although the main reason law firms are targeted is for financial gain, there is also a growth in bad actors using cyber-attacks to achieve political, economic or ideological goals.[3]

HR & Recruitment

Payroll fraud, recruitment scams, corporate espionage – cyber-attackers have found numerous routes into organisations via HR. Any identifiable information is valuable to criminals, and payroll and other HR systems are a treasure trove of names, addresses and bank details. If this is compromised, not only can it affect individual employees, it also gives attackers more ammunition with which to increase the likelihood of a successful attack on other parts of the business.

Additionally, recruitment agencies are prime targets for malware. If hit by a data breach, employment agreements and sensitive documents such as passport scans and visa details are all left exposed.

Manufacturing

The manufacturing sector, which includes automotive, electronics, and pharmaceutical companies, has always been a vulnerable industry when it comes to cyber-crime and security breaches. This is because intellectual property is incredibly valuable, and often manufacturing firms rely on highly specific software packages that are difficult to patch against recent exploits, making them highly vulnerable to attack.

Financial

The threats facing organisations working directly and indirectly with the finance sector go far beyond simple theft. Cyber threats facing banks, insurance companies, asset managers and similar organisations range from basic consumer-grade malware all the way up to highly targeted attacks from organised criminals and state-sponsored actors. Financial service providers are a hacker's favourite, given the nature of the private information held by those organisations.

[3] https://www.ncsc.gov.uk/report/-the-cyber-threat-to-uk-legal-sector--2018-report

Consultancy and support to allay cyber security concerns

Callsafe Services provides health and safety consultancy and training, predominantly within the construction industry, and has been an OGL Computer customer since 2009. With the increase in cyber-attacks, the company was keen to explore security improvements for their business. In 2017 Callsafe started to work with OGL Computer's sister company, CyberGuard Technologies.

Dave Carr, Managing Director of Callsafe, was happy to explain the reasons why they felt they needed to upgrade their security: "We were fully aware of the security threats that could harm our business and wanted to take a proactive approach in tackling cyber-crime. We needed an external company to provide professional support and advise on security issues facing our hardware and software. We wanted a company that was familiar with our needs and who could respond quickly to concerns and advise on security solutions. CyberGuard ticked all the boxes.

"Our IT security was previously only managed by a single password and wasn't exactly secure. CyberGuard Technologies advised how easy it was to access data with a single password and recommended Multi-Factor Authentication. This is where our security has benefitted the most, and now we are safe in the knowledge that our laptop users have significantly greater data security, satisfying our need to secure personal and client data stored on our laptops."

Callsafe invested in a state-of-the-art, next-generation anti-virus product called Carbon Black Defense, which not only looks for known viruses and malware, but also inspects threats by reviewing employees' behaviour. This deeper level of inspection enables CyberGuard Technologies to spot complex threats that would normally go undetected.

CyberGuard Technologies also helped Callsafe become Cyber Essentials compliant, as the team thought it was important to be accredited to provide evidence of the commitment to working securely.

> "Cyber security has been front of mind for SME customers for some time now, as awareness of cyber-risks continues to rise. Proactive management of IT requirements is in many ways connected to this trend, as businesses of all sizes look to compliance requirements as well as asset protection and disaster recovery. We've seen a real spike of interest in gaining actionable insights from business data too..."
>
> Colin Dennis, Head of Technical Operations, OGL Computer

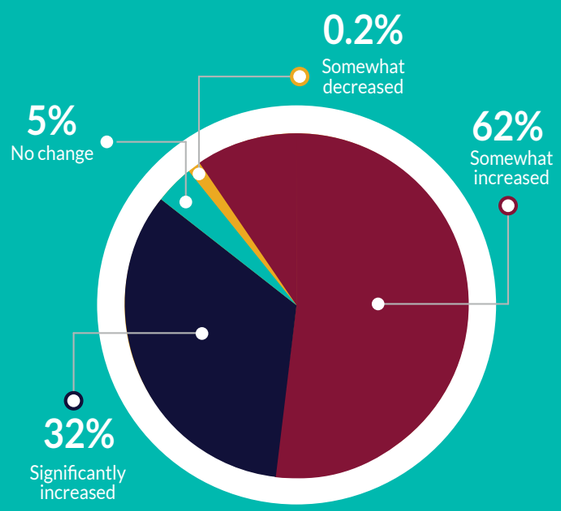
OGL Computer

Changing spend on IT / cyber security in 2020

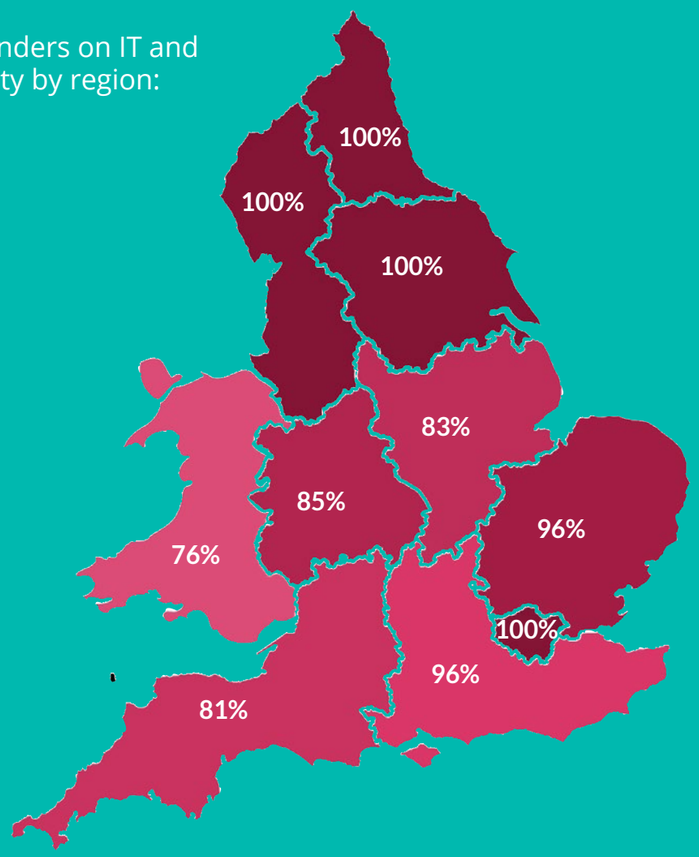
In the face of rising awareness of cyber threats and opportunities that technologies offer SMEs, it comes as a welcome confirmation that action is indeed being taken by UK SMEs in response.

The vast majority of SMEs (92%) plan to increase their spend on IT / cyber security, which is often budgeted as a single unit. To further support this positive investment in technology, a mere 5% expect the level of investment to stay the same, and just 1 respondent expects a decline in budget allocation.

Across all sectors, SMEs with 100 - 249 employees are most likely to increase IT budgets in 2020. Healthcare, HR / recruitment and manufacturing sectors were most likely to increase spend, while their peers in the legal, finance, retail and leisure sectors were least likely to increase spend.



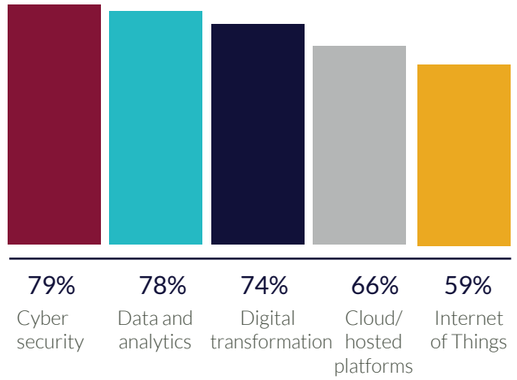
Highest spenders on IT and cyber security by region:



Plans for adoption of new and emerging technologies

SMEs have long recognised the opportunities technology provides to foster growth and improve profit margins, so appetites for new and emerging technologies are strong. The survey shows that while SMEs are familiar with, and implement mainstream technology, they also plan to invest in emerging technology.

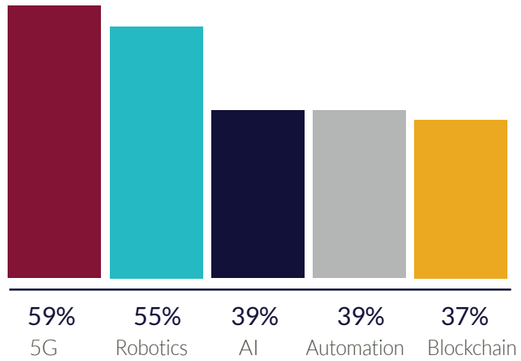
Top five technologies currently used by SMEs:



In context of the wider report that shows a key priority for 2020 being to increase cyber security provision (39%) and showing cyber-attack as a top concern (67%), the implementation of cyber security technologies (79%) is entirely consistent.

Interestingly 78% of UK SMEs are already familiar with managing data and analytics, while digital transformation also makes a strong showing. SMEs are using these to become more productive and efficient, providing a competitive advantage, and boosting both sales and revenue.

Top five new and emerging technologies SMEs plan to adopt:



> “For our company, a proactive IT strategy means ensuring we are using the most up to date and efficient systems, that fit our business. We equate efficiency with profitability, that’s why IT is at the heart of our business.”
>
> Marcus Gregory, Bluestar Leasing

With 5G networks really establishing themselves in 2020, 59% of businesses are planning to adopt this technology in order to stay ahead of competitors and use its full potential.

For SMEs, any gain in productivity can have a huge impact - hence the interest in robotics, with 55% planning to adopt the technology. While full-scale robots can be expensive, large and complex to install, a new generation of collaborative robots (or “cobots”) is changing the game for smaller companies by working alongside humans helping to complete tasks more effectively, offering new opportunities for employees, and even improving worker safety.

OGL Computer

Rather than a fully autonomous assembly line, a cobot performs a certain task that would help the operator with their job. For example, a cobot arm sorts and arranges cups of different sizes in an organised manner, making it easier for a human worker to attach the right sized handle to the respective cups.

With 39% of SMEs planning to adopt automation technologies, it's clear that offerings such as Robotic Process Automation (RPA) are becoming more popular to remove the burden that cumbersome manual processes and repetitive tasks can have on day-to-day business operations. SMEs can potentially benefit from a low-cost, accessible way to understand their data faster, enabling them to make better and more informed decisions. Especially as RPA can now be provided as a SaaS (software-as-a-service) offering.

Some analyst firms have predicted that UK GDP will be up to 10% higher by 2030 as a result of AI – the equivalent of an additional £232 billion – making it one of the biggest commercial opportunities in today's fast-changing economy[4]. While some SMEs are still not sure about potential use cases of AI for them, 39% of SMEs are planning to adopt the technology, with many innovative SMEs significantly cutting costs and delivering improved customer experience with AI-powered applications, which can be used for a range of tasks including automation, improved customer communication via chatbots and AI-powered personal assistants, saving time and improving email efficiency.

Blockchain has the potential to offer many benefits to SMEs, with 37% planning to adopt the technology for benefits such as trust, speed, increased safety and security as well as risk reduction in terms of less identity fraud and hacking, thereby reducing time and unnecessary costs. Blockchain is also a powerful supply chain automation tool, enabling the use of smart contracts to automatically manage processes that are currently manual.

> "AI technologies are mainly used for intelligent automation and acceleration of various complicated tasks and processes, and together with Machine Learning, they are helping to fight cyber criminals.
>
> Take for example, Kaspersky Threat Intelligence – a service that offers global intelligence from hundreds of sources. Using machine learning and artificial intelligence, it produces high quality threat data.
>
> Next-generation anti-virus product Carbon Black Defense helps protect user endpoints by not only looking for known viruses and malware, but also inspecting files and identifying threats by analysing previous user's behaviour. This deeper level of inspection allows CyberGuard Technologies to spot smart and complex threats that would normally go undetected."
>
> Scott Willmott, Head of R&D, OGL Computer

[4] https://www.pwc.co.uk//economic-services/assets/ai-uk-report-v2.pdf

Remote Working

Building a remote workforce can slash overheads, increase productivity, and improve employee efficiency, as well as boosting employee job satisfaction levels. This, in turn, can translate into better customer experience and increased profits.

Remote working can relieve some of the pressures of office life and reduce the costs at the same time, all of which goes some way to explaining why 94% of SMEs are seeing a growth in the number of remote workers employed and are turning to technology to support them.

- Strongly agree 54%
- Somewhat agree 40%
- Neither agree nor disagree 74%

With 50% of the respondents currently using technology and 34% planning to adopt technology enabling increased remote working, more progressive virtual tools, such as virtual reality conferencing, may become the preferred form of communication – even over face-to-face meetings. AI will also likely play a major role in managing remote staff.

> "Through remote workforce technology, our commercial team can work and access our business systems from anywhere in the UK and Europe if required. It means we can be consistent and efficient in our reporting and communications across the business."
>
> Ian Wright, Managing Director, SDI Displays

> "Hosted desktops used for remote working are much easier to manage than multiple PCs that all need their own applications, software upgrades and licensing. For IT teams, a central dashboard from which user permissions can be set and admin tasks carried out simplifies management tasks significantly."
>
> Steve Bennett, Strategic Solutions Architect, OGL Computer

For SMEs, building a remote workforce makes perfect sense. Thanks to changing attitudes and ever-improving network capabilities, it is predicted that half the UK workforce is expected to be working remotely by 2020[5].

Cloud-based products like Microsoft's Office 365 can keep employees connected from anywhere with a reliable internet connection and can offer them full access to workplace tools such as Word, Excel, PowerPoint, OneNote, Outlook, Publisher, and Access. Additional collaboration tools such SharePoint and Teams also enable easy file sharing and team working amongst employees in different locations.

[5] https://smallbusiness.co.uk/half-uk-workforce-remotely-2020-2540827/

Driving greater business efficiencies and profitability

OGL's State of Technology at UK SMEs survey uncovered the top three ways that SMEs plan to drive business efficiencies and profitability via technology:

- Increasing the use of collaboration tools such as Microsoft Office 365, Teams, SharePoint etc **59%**
- Increasing the adoption of cloud computing **57%**
- Investing in effective backup and disaster recovery solutions to ensure business continuity **55%**

Deviating from these figures were the following with different top priorities:

- Automating business processes in line with a digital transformation strategy was a key driver for the healthcare sector **63%**

And those choosing investment in effective backup and disaster recovery solutions to ensure business continuity were:

- Companies with 100-249 employees **56%**
- SMEs with an average annual turnover of £50-£99.99 million **59%**

Enterprise-grade strategic solution designed for new customer wanting to go virtual

Joseph Ash Galvanizing is a UK leader of steel finishing services including galvanizing, spin galvanizing, engineering, shot blasting and powder coating.

With 500 employees and eight plants in the UK, they serve all types of customers from large construction companies and fabricators, to fencing and agricultural specifiers, government departments and even metal sculpture artists.

> "In working with OGL we have been able to upgrade our systems at a quicker pace than would have been possible doing the work in-house. Because of the excellent professionalism of OGL personnel we have been able to 'learn as we go' about the new systems during implementation. Their staff took care to spend time with us explaining and educating our internal IT resource which has been invaluable."
>
> Mick Jackson, Head of IT & Marketing, Joseph Ash Galvanizing

Joseph Ash solution features include:

Replacement firewall

A new firewall has been implemented, specifically engineered for mid-sized and distributed enterprises, to replace the existing device to enhance security, improve management and to provide a level of high availability (HA). An excellent solution in the face of an explosive growth in bandwidth rates, encrypted traffic, video use and connection speeds.

Powerful security

Best-of-breed security components and software from WatchGuard underpin the Joseph Ash solution throughout and offer boosted protection in critical attack areas across the infrastructure.

Office 365

Microsoft Office 365 will provide business-class email, calendar and contacts delivered to employees' PCs, phones and browsers. New levels of reliability have been achieved whilst also ensuring protection of sensitive and confidential information.

Backup

A localised NAS device was implemented at head office with Veeam backup and replicated software to backup the local server estate. One of the existing host servers was moved to a second Joseph Ash site where it became a disaster recovery target using Veeam Cloud Connect. This enhanced the backup routine and built in a level of disaster recovery to complement the local VM backup images.

Virtualised infrastructure

A solution designed around two Hewlett Packard host servers running VMware Hypervisor as a mature virtualisation platform. Designed to provide a centralised management system enabling the internal IT team to manage their entire server farm from a single console thereby improving efficiency, performance and productivity.

New server hardware

Servers from the Hewlett Packard DL series are versatile, rack optimised and have a balance of efficiency, performance and management, designed with scalability in mind, enabling dual processor capability.

Securely moving to the cloud

In spite of their familiarity with cloud technology, a sizeable 76% of UK SMEs are nervous about moving from an on-premise IT infrastructure to a cloud infrastructure, due to concerns over data security.

While there are challenges involved in moving to a public cloud environment, preparation and planning will mitigate most effectively. However, it is essential that internal data policies are implemented in the cloud, and / or cloud providers are compliant with required industry standards on data security.

> “Many SMEs are scared to move to the cloud because they feel uneasy with data being held off-site and not having control of their hardware.”

Nicola Smith, Director, Star Fasteners

Nervous about moving from on-premise to cloud due to data security fears?

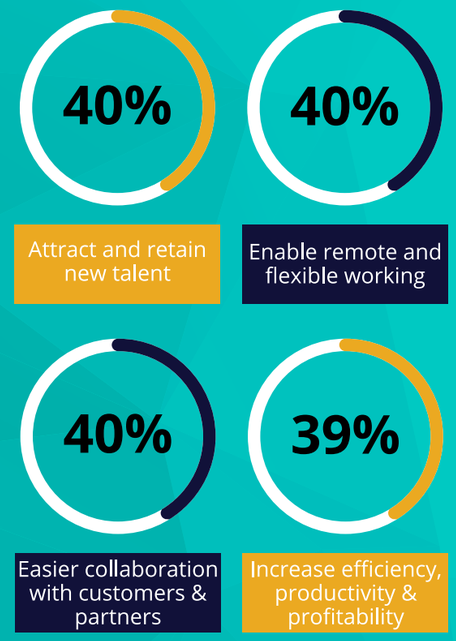
> “Cloud solutions have matured significantly over the last few years, so there will be several offerings that suit your business to a tee – just ensure that your wish list is full and complete and ensure due diligence is conducted.”

Scott Willmott, Head of R&D, OGL Computer

Reasons for adoption of new technologies

The drivers behind new technology adoption for UK SMEs shone through loud and clear, with just over half (51%) stating that cyber security threats were the biggest reason, beating even competitive advantage which came in second at 44%.

Attracting and retaining new talent at 40% was neck-and-neck with enabling remote and flexible working at 40%, and also with facilitating collaboration with customers and partners at 40%, a strong indicator of the value placed on a skilled workforce and good communication.



> “We will look at each technology on its own merit, to see if it benefits our business. We have no immediate intentions to change everything, but working with OGL Computer, we want to keep moving with the times.

The main reason for adopting new technologies is to be as efficient as possible. As long as it is secure and provides a business efficiency then it’s worth trying. It has to be right for our business though.”

Ian Wright, Managing Director of SDI Displays

About the Study

In November 2019, OGL Computer surveyed senior executives with decision-making authority for technology products and services at 405 SMEs, ranging in size from 50 to 500 employees across a number of vertical sectors.

Further interviews were used to explore opportunities, threats and strategies with the following SME executives:

- **Ian Wright, Managing Director, SDI Displays**
- **Mick Jackson, Head of IT & Marketing, Joseph Ash Galvanizing**
- **Dave Carr, Managing Director, Callsafe Services**
- **Nicola Smith, Director, Star Fasteners**
- **Marcus Gregory, Director, Bluestar Leasing**
- **Rob Samuel, IT Manager, IntaPeople**

> “One of the key considerations when developing a cyber security strategy is understanding the potential attack surface hackers have access to – we may guard our key business and financial systems, but employees are also vulnerable to social engineering. We need to ensure we are protected on multiple levels and be proactive in all areas of cyber security.”
>
> Rob Samuel, IT Manager, IntaPeople

About OGL Computer and CyberGuard Technologies

About OGL Computer

OGL Computer is the technology partner to over 1,200 UK businesses, including small, growing businesses as well as multi-site enterprise businesses. We are accredited by the world’s leading IT and cyber security vendors, to deliver best-in-class IT, business software and cyber security solutions. We are incredibly proud of our 40-year heritage and our unique proposition whereby our three specialist divisions work closely together to deliver the complete technology package to our customers.

OGL Computer is the author and developer of fully integrated ERP software solutions for stockists, distributors and wholesalers across the UK. OGL Software offers a wide range of modules including: CRM, Sales Order Processing, Warehouse & Stock Management, Accounts & Invoicing, Sales Analysis and eCommerce integration, which takes care of all common business processes to deliver greater efficiency and profitability. OGL Software is the premier choice for organisations looking to drive their business forward.

CyberGuard Technologies

CyberGuard Technologies (an independent company within the OGL Computer Services Group) provides the very best in IT security for UK businesses looking for premium IT performance in a protected, secure environment. Our cyber defences protect against the potential devastation of an attack from cyber-criminals including defending your finances, identity, reputation, data and your customers’ confidential information.

We protect our customers from end-to-end through; Security Testing, Managed Detect & Respond Services, Security Awareness Training and Cyber Certification, and provide reassurance in the event of an attack through fast and effective Cyber Incident Response, built upon sound threat intelligence gathered by our own team of cyber analysts coupled with intel from various global sources.

OGL Computer

Get in touch

Find out more at enquiries@ogl.co.uk or call us on 01299 873 873

ogl.co.uk

cg-tech.co.uk