



The SME Cyber Security Report

Making Cyber Security Accessible for Small Businesses

Created By:
AdaptiveComms

 **AdaptiveComms**
Phones | IT | Cyber | Data Networks | WiFi

SELF ASSESSMENT

This self-assessment will help you understand your business's current setup and infrastructure. If your answers are **mainly positive**, go ahead and **leave the paper!** You **don't** need to read on.

Questions	Answer
How Long Could You Operate WITHOUT Your Computers?	
How Much Money Would You Lose a Day if You Couldn't Operate?	
How Long is That Sustainable?	
How Many Customers do You Think Would Buy Elsewhere if You Weren't Able to Provide Them Your Goods/Services?	
How Many Customers Would Come Back?	

SELF ASSESSMENT

Questions	Answer
What Reputational Damage Would an Attack Cause You and Would That Cost New and Returning Customers?	
How Long Did It Take You to Earn the Money You Could Lose?	
How Much Is it Worth to You to Pay to Protect Yourself Against That? (Don't Tell Us)	

Thank You for Completing Our Cybersecurity Self Assessment!

As you read ahead, please keep your answers in mind.

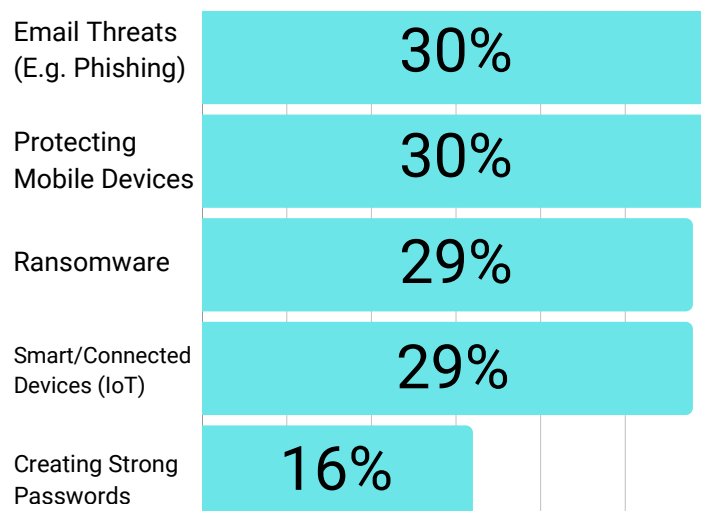


Understanding Cyber Security

Cyber attacks have rapidly emerged as a major threat to businesses, with recent discussions suggesting that the financial impact and damage they inflict are now a **greater risk than burglary**.

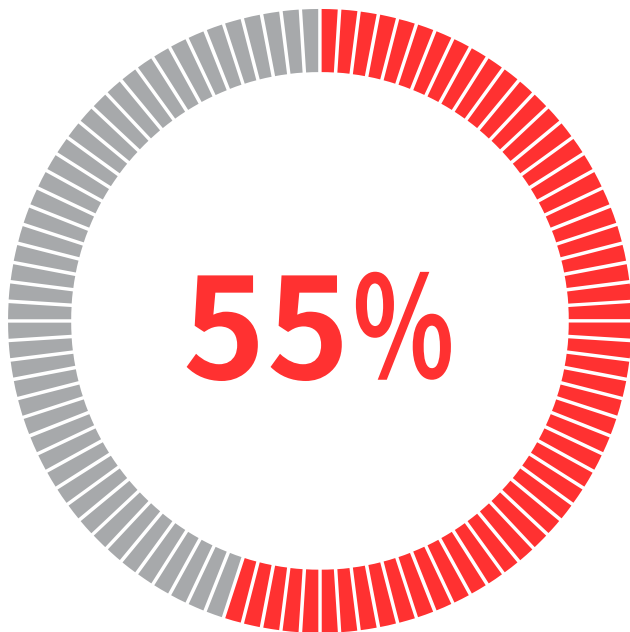
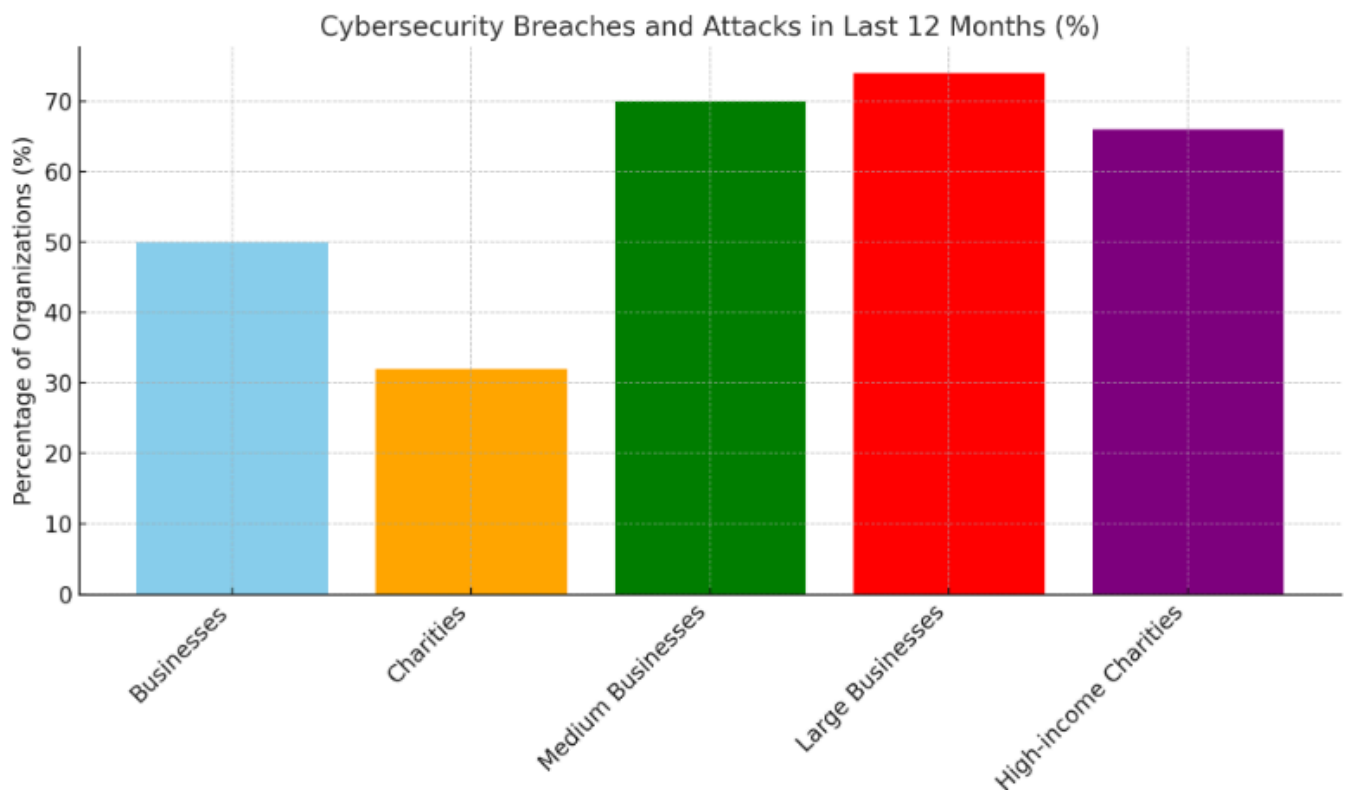
In what feels like an instant, the need to improve your cyber security posture has shifted from a concept in sci-fi movies to a critical component of business protection. Most business owners know the importance of cybersecurity and want to do something about it, but they just **don't know how**.

Where Do People Think Their Own Cyber Knowledge Gaps Are? ^[1]



CYBERSECURITY BREACHES 2024

Official stats from the UK Government's Cyber Security Breaches Survey 2024.^[2]



COMPANIES NEVER
RECOVER FROM A
CYBER BREACH.^[3]

Where To Turn?

With cyber threats now so abundant and constantly changing, business owners and decision makers find it challenging to know how to respond and where to seek help from.

CURRENT CYBER SECURITY THREATS YOU SHOULD KNOW

We have outlined some examples of easily available hardware or software used by the criminals and nation states involved in hacking business (we haven't published specific "brand" names to avoid helping the criminals).



Cloning Physical Assets

A device available online for **£21.45**, including delivery, can clone various types of entry cards, such as:

- Workplace access fobs
- Hotel room keys
- Credit cards
- Certain smart car keys



AI & DeepFakes

A recently reported incident highlighted the use of deepfake technology by a criminal who obscured their own face and voice, assuming the identity of a CEO.

This manipulation successfully persuaded an employee to transfer funds into the perpetrator's account.



Trojan Software

Several types of Trojan software exist, with one common variant capable of disguising phone numbers and intercepting text messages. This malware can access and upload personal data, including facial and financial information, enabling data theft. It also intercepts two-factor authentication messages and alerts, creating serious security risks.



Email Attacks

We have all come across spam emails in our inboxes and quickly deleted them. However, these messages are evolving to become more sophisticated, capable of tricking even the most cautious users. Once you interact with them, they frequently act as a confidence scam or install covert software on your device, enabling them to track your screen and keystrokes, e.g. granting bank access.



Port/Vulnerability Attacks

Cyber attacks on SMEs are increasingly common and can have severe consequences. State-sponsored hackers use AI-powered bots to identify vulnerable routers and firewalls. Once vulnerabilities are found, hackers attempt to infiltrate systems, shut them down, and demand a ransom. If payment is not made, sensitive information may be sold on the dark web, rendering digital operations unusable.



Website Attacks

A widely used tool among hackers, these attacks can exploit vulnerabilities found in web plug-ins, granting them access to your e-commerce site or customer data.

Last year, the UK experienced **17,900** of these attacks, and the number continues to rise.

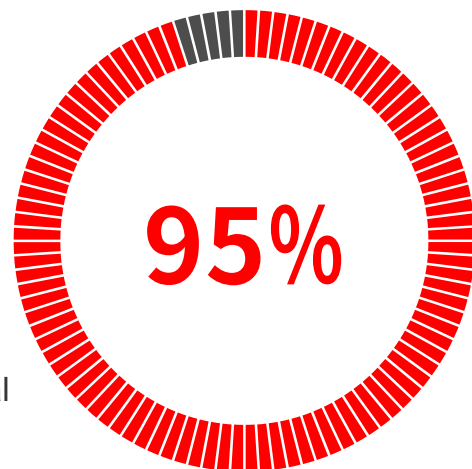


Human Error

Human error accounts for a staggering **95%** of reported attacks.^[4]

In other words, if human error was somehow eliminated, **19 out of 20 cyber breaches may not have taken place at all!**

Employees at organisations lacking training, weak information security policies, and minimal protective applications are highly vulnerable, making them the primary targets for exploitation.



The Impacts of a Data Breach



\$4.88M
(£3.87M)

The overall global cost of a data breach in 2024—a **10% increase** over last year and the highest total ever. ^[5]

60%
Revenue
Loss

60% of customers are hesitant to engage with brands that have experienced a data breach. Only **10% feel protected by these brands**, while **48%** reported their personal data was **left vulnerable** due to **inadequate protection** following such breaches. ^[6]

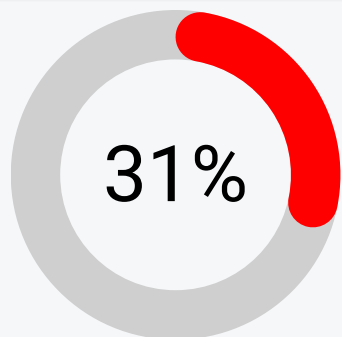
£30,000
to £10M

In 2023, the ICO imposed **17 fines** ranging from **£30,000** to over **£10 million**, with 9 under **£100K** and 8 above. These fines totaled over £13 million, with an average fine of **£816,471**, nearly double the 2022 average. ^[7]

£21,000

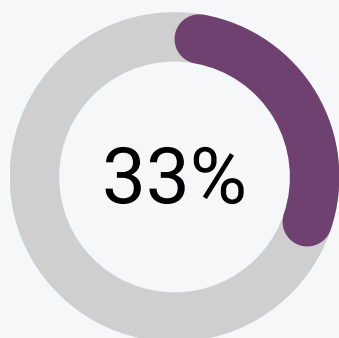
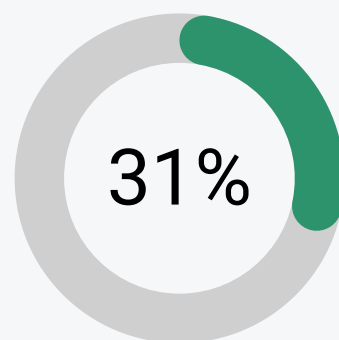
Cyber attacks pose significant risks to businesses, costing an average of £21,000 in remediation fees. In the UK, small businesses are particularly targeted, with two-thirds of companies employing 10-49 staff experiencing cyber-attacks in the past year, totalling around 130,000 businesses affected. ^[8]

Loss of Customers, Employees, and More



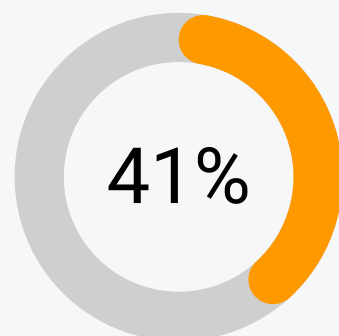
In the past year, **31%** of data breaches resulted in job losses. These losses may stem from the dismissal of IT or security personnel, or they could be part of broader layoffs caused by business disruptions.^[9]

Almost a third (31%) of global organisations suffered a breach of data in their SaaS applications last year, as they struggled to gain visibility and control over their cloud environment.^[10]



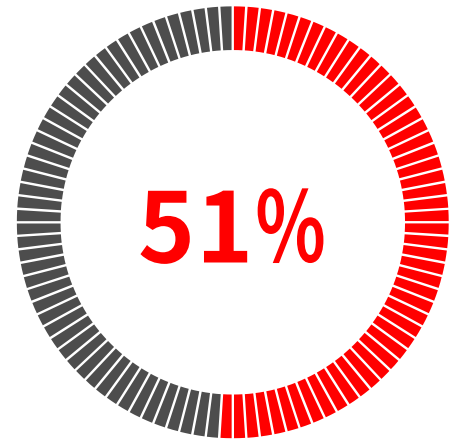
One-third of consumers globally have experienced a data breach. Such incidents can greatly affect consumer trust in online organisations and decrease the likelihood of them continuing to engage with the business afterward.^[11]

Consumer research has also found **41%** say they'll **never return** to a business after a security issue and **44%** say they'll **stop spending** at least temporarily.^[12]



No Cybersecurity

We're living in a time where many business owners are aware of the dangers of cyber attacks and want to do something about it, but they often feel a bit lost on where to start. Most cyber security solutions seem geared towards big companies with deep pockets, which just isn't realistic for everyone.



51% of small businesses have no ^[13] cybersecurity measures in place at all

What Do I Do?



Consider a vCIO!

vCIO stands for **Virtual Chief Information Officer**, providing the same consulting services and responsibilities as an in-house CIO, but remotely.

Organisations prefer vCIOs to improve cyber security without needing a full in-house team.



TRUSTED TECH CONTACT WITHIN YOUR BUSINESS

We want to create a strong, productive and personal relationship with you, your staff, and your business. We want to align our paths to the same goals.

AFFORDABLE SOLUTION FOR YOUR BUSINESS

Not all businesses can have a full in-house IT team, yet the need for quality technology is rising. Having a vCIO allows you to achieve your IT goals without a complete team, providing predictable monthly costs through managed service providers.

TECHNICAL REPORTING DONE FOR YOU

Technical reporting is crucial for a vCIO, providing a quarterly opportunity to evaluate and respond to organisational goals. This reporting assesses key areas such as:

- Compliance Needs
- IT Projects and Expenses
- Support Metrics and Satisfaction
- Project Status
- Relationship Health

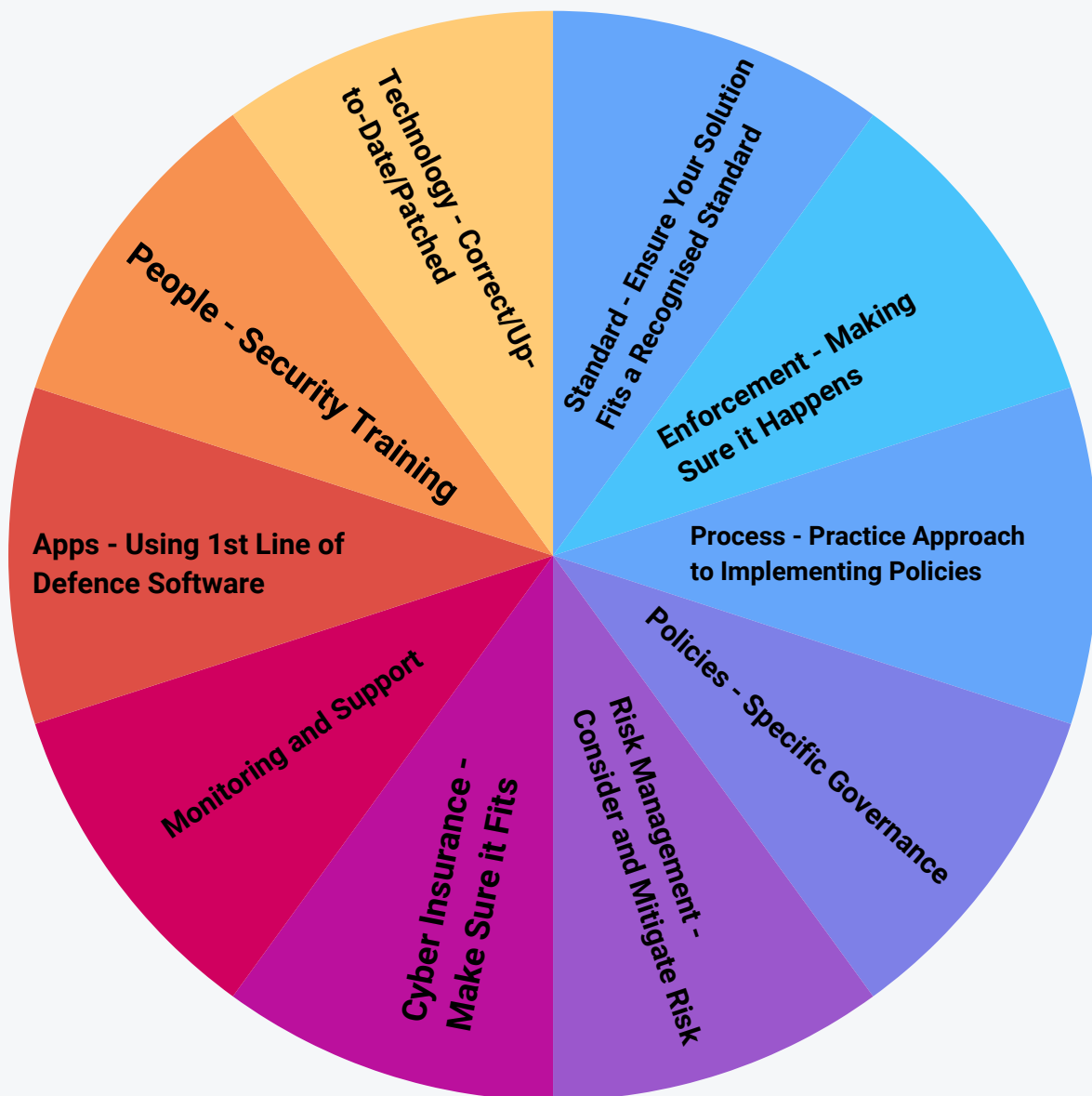
DEFINE IT OBJECTIVES AND PLAN THE TECHNOLOGY ROADMAP

Planning your organisation's technological future is vital for a valuable vCIO during digital transformation. We help set long-term direction and informed decisions. Key issues addressed include:

- Intellectual Property Protection
- Disaster Recovery
- Employee Onboarding
- Cyber Security Training

Which Cyber Security Protection is Right for Me?

When looking to enhance an organisation's cyber security posture, it's crucial to recognise that cybersecurity protection is not a one-size-fits-all solution. There are multiple components to consider when establishing a robust first line of defense in cyber security.



AdaptiveComms Approach to Cyber Security



We know SME owners and managers are very serious in wanting to protect their staff, customers, the business' wealth, IP and Commercially sensitive secrets. They want to have the peace of mind that they are doing all they reasonably can to protect everything they have built.

We also know that 1st line defence cyber security can appear out of reach for many SMEs because it appears to be the realm of the corporate. But with AdaptiveComms 1st line of defence cyber security package you too can have approved protection. Our cover uses the power of cloud computing to democratise the apps and offer enterprise level solutions to SMEs for a "by the user" monthly cost.

AdaptiveComms is dedicated to bringing its client's cyber security readiness up to a specified and accredited level to ensure they are fully protected to NIST framework standards. We do this by using a thorough and methodical approach to bringing your system and processes up to the correct standards, de-mystifying the work needed to be done.

Your Cyber RoadMap

FIRST CONSULTATION

- Assess Where You Are
- Implement Various Procedures
- Implement Hardware & Software
- Provide You with a Clear Understanding of What You Need to do to Maintain the Internal Process Elements of the Keeping it Going

1

INSTALLATION

- Select and Configure Your Cybersecurity Tools e.g. Firewall, Detection/Prevention Systems, Endpoint Protection and More.
- Implement Network and Device Security Controls
- Deploy Monitoring Systems
- Conduct Testing and Quality Assurance
- Document Installation and Train Team Members

2

AFTER INSTALLATION

- Ongoing IT User Support
- A Quarterly Business Review - tracking a roadmap to bring you to the highest standard and maintain it, allowing you to budget for the future
- A standing watch on your systems monitoring for attacks with packages available on a 24/7.365 basis

3

8/5 ACCESS TO OUR TEAM

- A vCIO to Plan and Advise on your IT and Cyber Strategy
- Access to the IT support team to keep the day to day IT running smoothly
- Monitoring from the cyber watch team as well as access to our 24/7/365 MDR monitoring team to watching for and responding to threats as they happen

4

Pricing Starts at £65 Per Month Per User

Includes:

- ✓ AntiVirus
- ✓ IT Support
- ✓ Response and Detection
- ✓ Full Suite of Cyber Security Products
- ✓ Firewall
- ✓ Security Awareness Training

Your Cyber RoadMap

FIRST CONSULTATION

- Assess Where You Are
- Implement Various Procedures
- Implement Hardware & Software
- Provide You with a Clear Understanding of What You Need to do to Maintain the Internal Process Elements of the Keeping it Going

1

INSTALLATION

- Select and Configure Your Cybersecurity Tools e.g. Firewall, Detection/Prevention Systems, Endpoint Protection and More.
- Implement Network and Device Security Controls
- Deploy Monitoring Systems
- Conduct Testing and Quality Assurance
- Document Installation and Train Team Members

2

AFTER INSTALLATION

- Ongoing IT User Support
- A Quarterly Business Review - tracking a roadmap to bring you to the highest standard and maintain it, allowing you to budget for the future
- A standing watch on your systems monitoring for attacks with packages available on a 24/7.365 basis

3

8/5 ACCESS TO OUR TEAM

- A vCIO to Plan and Advise on your IT and Cyber Strategy
- Access to the IT support team to keep the day to day IT running smoothly
- Monitoring from the cyber watch team as well as access to our 24/7/365 MDR monitoring team to watching for and responding to threats as they happen

4



What Our Clients Say:

Southport Hotel

Chief Engineer

Fantastic company to support your business. As a medium/large-sized hotel, we require a reliable IT support company, and AdaptiveComms has been exceptional for more than 8 years with us. They have thoroughly covered all aspects of our cyber security and maintain a friendly team ready to help at any time.

I highly recommend AdaptiveComms in Southport for their expertise and the sense of security they provide when assisting with any issues, installations and repairs.

St Catherine's Hospice

IT Manager

AdaptiveComms made consolidating our business mobiles effortless.

Their quick and attentive local support made us feel highly valued as customers.

It's been a great experience working with them.

North West Air Ambulance Charity

IT Manager

We have been customers of Adaptive Comms for 4 years now, and they always provide excellent levels of service.

The phone system itself is reliable and feature rich, offering us services that assist our teams on a day-to-day basis. The system has developed well over the years and new features are continually added, along with improvements to the phone app.

I would highly recommend AdaptiveComms.

Manchester Secondary PRU

Business Manager

Words cannot express how grateful I am for AdaptiveComms - the change has been incredible!

The engineers knew exactly what to do to help our organisation and reduce our costs massively, and continue providing ongoing support whenever we need them.

St Helen's Coalition of Disabled People

Charity Co-Ordinator

Our systems at the St Helens CDP were extremely outdated so we needed to totally update them.

The service we receive is excellent, our Wi-Fi is faster than ever and if we have any issues we find the team are so helpful and quick to fix.

I'm glad we decided to work with AdaptiveComms.

Options for Supported Living

Operational Development & Innovation Manager

What felt like a daunting task turned out to be a smooth operation for the team at AdaptiveComms.

The engineers did an amazing job, the system works great and nothing was a problem.

Any problems we do have however are fixed in a flash!

Southport Market

Operations Officer

AdaptiveComms provided a thorough service from start to finish and helped the Market get quickly connected and on it's feet again ready for a fresh new face of customers.

The engineers did a fantastic job surveying and installing the equipment with little to no disruption in line with our refurbishment schedule. Would highly recommend!

Southport Air Show

Events Officer

For a third year in a row the Southport Air Show has been a huge success thanks to the incredible work from AdaptiveComms.

The engineers were brilliant as always, 100% reliable and the service was top notch.

Swansway Motor Group

Director

AdaptiveComms has been a supplier for over 20 years, they now handle all our telephony and related DR across 25 sites. After reviewing the market there was no-one else I felt was able to provide the right mix of service, quality and technical know-how. They have proved knowledgeable, and they just make it work. With over a thousand staff, I need to be able to rely absolutely on our communications provider, and I can.

AdaptiveComms have proved an able, agile and reliable partner.

Clifton Trade Bathrooms

Director

Words cannot express how grateful I am for AdaptiveComms - the change has been incredible!

The engineers knew exactly what to do to help our organisation and reduce our costs massively, and continue providing ongoing support whenever we need them.

St Helen's Coalition of Disabled People

Charity Co-Ordinator

Our systems at the St Helens CDP were extremely outdated so we needed to totally update them.

The service we receive is excellent, our Wi-Fi is faster than ever and if we have any issues we find the team are so helpful and quick to fix.

I'm glad we decided to work with AdaptiveComms.

Options for Supported Living

Operational Development & Innovation Manager

What felt like a daunting task turned out to be a smooth operation for the team at AdaptiveComms.

The engineers did an amazing job, the system works great and nothing was a problem.

Any problems we do have however are fixed in a flash!





01704 540547



info@adaptivecomms.co.uk



www.adaptivecomms.co.uk



AdaptiveComms
Phones | IT | Cyber | Data Networks | WiFi

[1] <https://www.eset.com/us/infographic-employees-and-cybersecurity-the-knowledge-gap/?srsltid=AfmB0opK3U8zmNAGDjFHPYwgeB474myCioMziS2gSryaifhPt87nF>
[2] <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024>

[3] <https://www.fuellednetworks.com/55-of-smba-close-down-within-6-months-of-a-cyberattack-invest-in-asset-management-now-before-its-too-late/>

[4] <https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches>

[5] <https://www.ibm.com/reports/data-breach>

[6] <https://chainstoreage.com/how-do-consumers-react-security-breach>

[7] [https://www.umnconsulting.com/blog/analysis-of-fines-imposed-by-the-information-commissioners-office-in-2023/#~:text=The%2017%20fines%20imposed%20by%2C%20IT%20K%20\(see%20below\),](https://www.umnconsulting.com/blog/analysis-of-fines-imposed-by-the-information-commissioners-office-in-2023/#~:text=The%2017%20fines%20imposed%20by%2C%20IT%20K%20(see%20below),)

[8] <https://www.madeinbritain.org/news/uk-small-businesses-hit-hardest-by-cyber-attacks/#~:text=Cyber%20attacks%20can%20be%20detrimental%20for%20businesses%2C%20with%20the%20average%20cost%20to%20remedy%20an%20attack%20being%20%2C%20A%201%20C000>

[9] <https://www.dclsearch.com/blog/2018/09/31-percent-of-cyber-attacks-lead-to-job-losses?source=google.com>

[10] [https://www.infosecuritymagazine.com/news/third-organizations-saas-data/#~:text=Almost%20a%20third%20\(31%25\)%20cloud%20environments%2C%20according%20to%20AppOmni](https://www.infosecuritymagazine.com/news/third-organizations-saas-data/#~:text=Almost%20a%20third%20(31%25)%20cloud%20environments%2C%20according%20to%20AppOmni)

[11] <https://www.emarketer.com/content/33-of-consumers-victims-of-data-breaches-on-companies-that-tasked-with-keeping-their-data-safe>

[12] <https://www.businesswire.com/news/home/20190917005012/en/New-Global-Research-Shows-Poor-Data-Security>

[13] <https://www.strongdm.com/blog/small-business-cyber-security-statistics/#~:text=22%20rising%20fear%20of%20new%20threats.&text=30%20cybersecurity%20tools%20SMBs%20are%20adopting>