modernnetworks

TECHNOLOGY INSIDER

DECEMBER 2023

Your monthly newsletter, written for humans not geeks

Inside this edition

Cyber Security Strategy: Two Sides of the Same Coin

Cybersecurity is a vital aspect of any business. However, many organisations are still vulnerable to cyberattacks that can cause significant financial and reputational damage. In this blog, we will explore the two sides of a complete cybersecurity strategy: prevention and recovery plan. Prevention is all about the measures that your business can take to reduce the risk of a cyberattack, such as using strong passwords, encrypting data, and updating software. Recovery plans are the steps that can help your organisation recover from a cyberattack, such as restoring backups, notifying stakeholders, and investigating the root cause.

The cost of security failures

According to the UK government's official statistics for 2023, the average cost of a disruptive cybersecurity breach across all businesses was £1,100. However, this figure becomes greater as the size of a business increases. For medium and large enterprises, the average cost was approximately £4,960. Additionally, UK organisations took on average 181 days to discover a breach and a further 75 days to contain it. The same UK government report also clearly states that most cyberattacks could be prevented by taking basic security precautions.

Heads: it's prevention

The first half of a complete cybersecurity strategy involves taking steps to protect your business from cyber threats. This includes implementing measures such as firewalls, antivirus software, and intrusion detection systems. It also involves educating your employees on how to identify and avoid potential threats, such as phishing emails and social engineering attacks. By taking these precautionary steps, your business can significantly reduce its risk of falling victim to a cyber-attack.

Continues on the next page >>>

Prevention plans include:

- User education and security awareness training
- Robust access controls and authentication
- Regular software updates and patch management
- Network security and firewalls
- Regular security audits and vulnerability assessments
- On-going monitoring and support.

Tails: recovery

Despite taking all necessary precautions, there is always a possibility of a cyber-attack succeeding. This is where the second part of the strategy comes in - a recovery plan. A recovery plan is the other side of the same coin. It outlines the steps that your business will take to recover as quickly as possible in the event of an attack. This includes data backups, disaster recovery and incident response plans. By having a recovery plan in place, your organization can minimize the damage caused by an attack and resume normal business operations as soon as possible.

By implementing appropriate controls designed to strengthen data protection and improve security, you can reduce your organization's risk and lower its insurance premiums. Working together, a cyber recovery plan will help reduce the impact of an operational outage from weeks to hours or days, while cyber insurance will help cover the cost of any lost revenue during the recovery period.

Recovery plans include:

- Incident response plan
- Data backup and disaster recovery
- Forensic analysis and learning
- Legal and regulatory compliance
- Cyber insurance.

Don't leave things to chance

Cybersecurity is not a matter of chance, but a matter of choice. You should never leave your business's security to the luck of a coin toss, as the consequences of a cyberattack can be devastating. Instead, you need a cybersecurity strategy that is like two sides of the same coin. One side is the preventive measures that you can take to avoid becoming the victim of an attack, such as using strong passwords, encrypting data, updating software, and educating employees. The other side of the coin is the recovery plans that you should put in place, including insurance coverage, backup systems, and incident response teams, so you can quickly recover should the worst happen. By having both sides of the same coin, your business can reduce the risks and costs of a cyberattack and protect its reputation and assets.

To learn more about how Modern Networks can help you develop and implement a complete security strategy for your business, contact us now.

DID YOU KNOW...

not to download third party apps?

New research has found that an Android app is actually a trojan (a type of malware) that can record your video and audio calls. The SpyNote banking Trojan is typically delivered by a phishing SMS, and once installed, it's very hard to get rid of.

How do you avoid it? Simple. Only download apps from official app stores – never via third parties.

NEW TO MICROSOFT 365

Outlook could soon be writing your emails for you

Thanks to Copilot (Microsoft's AI companion), you'll be able to draft more concise, professional emails in Outlook, with suggested edits for clarity and inclusive language.

And if there's a long email thread you need to respond to, Copilot can even summarise it and draft suggested replies.

Important Update: Your Anti-Virus Protection is Being Upgraded

Dear Customers,

We are excited to announce that over the next three months, we will gradually replace your current Modern Networks anti-virus with a new underlying solution. This change will provide you with increased levels of protection, and the best part is that there will be no price change. You will not experience any impact on your service whatsoever, except for a change of icon in your taskbar.

As you can see below, the new anti-virus has more features and a higher malware detection rate than our existing anti-virus solution.

New MN anti-virus features

Risk Analytics Find and fix vulnerabilities, track & improve risk scores	**Exploit Defence** Detects exploit techniques, stops 0-day exploits
Web Threat Protection Behavioural traffic scan (incl. SSL), Anti-phishing, Search Advisor	**Behaviour monitoring** O-Trust process monitor automatically blocks malicious processes
Content Control Restrict user access to applications, sites or web categories such as gambling	**Network Attack Defence** Blocks network-based attacks such as Brute Force or Password Stealers
Device Control Control access and use of USB or other external devices.	**Firewall** Two-way host firewall protecting endpoints anywhere
	Ransomware Mitigation (New) Restore files after ransomware attacks from secure copies.

The new Modern Networks AV solution is a powerful and comprehensive security solution that will protect your devices from all kinds of threats. In addition, the introduction will enable you to progress to the Modern Networks MDR solution.

MDR stands for Managed Detection and Response, a service that provides 24x7 security monitoring, advanced attack prevention, detection and remediation, and targeted and risk-based threat hunting by a certified team of security experts.

With Modern Networks MDR, you get all the benefits of our award-winning platform, including endpoint detection and response, automated remediation, and host-based firewall and web control. Plus, you'll get the additional benefits of our Security Operations Centre (SOC) which will provide around-the-clock, following-the-sun, monitoring, prevention, detection, investigation, and response to cyber threats.

Continues on the next page >>>

The benefits of our MDR with SOC solution include:

- Improved risk management
- 24x7 security monitoring
- Advanced attack prevention, detection and remediation
- Targeted and risk-based threat hunting by our team of certified security experts
- Endpoint detection and response
- Automated remediation
- Host-based firewall and web control
- Access to our dedicated team of security analysts and threat intel researchers
- Regulatory compliance enforcement
- Exceed mandatory cyber insurance requirements
- Reduce costs.

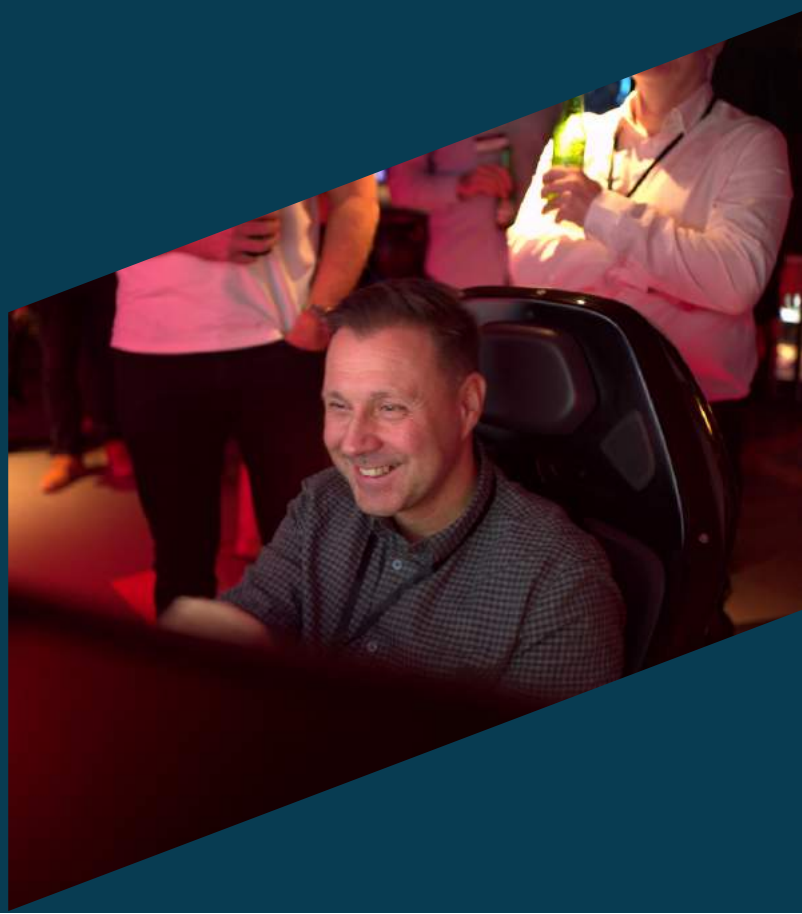
We are committed to providing you with the best possible security solutions, and we believe that Modern Networks AV and MDR with SOC are the perfect fit for your needs.

If you have any questions or would like to know more about improving your security posture, please contact your account manager now.

Modern Networks hosts a successful business development event at F1 Arcade, London.

We, at Modern Networks, recently hosted a fantastic business development event at London's F1 Arcade on the 23rd of November. Our event, named the "Pace of Digital Change, F1 Challenge," was a chance for multi-location SMEs, particularly in the warehouse, logistics, professional service, and commercial property sectors, to informally mingle with our team while enjoying the high-speed excitement of the F1 Arcade. The F1 Arcade is a state-of-the-art venue that offers realistic and immersive racing simulators, as well as a bar and lounge area.

We were thrilled to welcome over thirty guests to an enjoyable evening filled with drinks, snacks, and awesome F1 simulators. It was an opportunity for our guests to learn a little more about Modern Networks, and how our IT managed services can help businesses adapt to fast-paced digital transformation. Alongside networking, our guests had a blast competing in our F1 Challenge, racing on various tracks and cars using the simulators.



Wrapping up the evening, we announced our F1 Challenge winners, presenting them with some eye-catching trophies. Darren Wain, Harneys Fiduciary bagged first place. Lloyd Parker from Assured Digital Technologies took second place. Third place went to Luke Foad, MeldCX.

As the Senior Business Development Manager at Modern Networks, Jeff Wheeldon remarked: 'I can say that the event wasn't just about the fun of F1 simulators. It was a great opportunity for both existing and potential clients to connect with our team. The event also gave people an opportunity to discuss some of the challenges that businesses face today and how technology can help navigate a way forward.'

The event was successful in strengthening our relationship with our current clients and some potential new ones. It also provided us with a great opportunity to showcase our knowledge and expertise as IT and telecoms solutions providers. We would like to thank all the attendees for their participation and valuable feedback. Additionally, we would like to recognize our partners at TMW and the F1 Arcade for their excellent hospitality and service.

For more information about Modern Networks and upcoming events, **visit our website**. To discuss any new business requirements, call **01462 426500** or email **info@modern-networks.co.uk**.

OPENING HOURS

Dear Customers,

We will have a full team on the Service Desk providing tech support between Christmas and New Year:

- Friday 22nd December – 8am to 6pm
- Monday 25th December – Bank Holiday
- Tuesday 26th December – Bank Holiday
- Wednesday 27th December – 8am to 6pm
- Thursday 28th December – 8am to 6pm
- Friday 29th December – 8am to 6pm
- Monday 1st January – Bank Holiday
- Tuesday 2nd January – 8am to 6pm

Additionally, our Guildford office will be working 9am to 5.30pm throughout the festive period, except for the UK official Bank Holidays.

CHANGE FREEZE

We would like to inform you that there will be a change freeze period from the 15th of December 2023 until January 3rd, 2024. This means that no changes will be made to your IT systems or services during this time unless they are urgent or pre-approved.

Why are we doing this?

We want to ensure that your IT systems and services are stable and secure during the holiday season when many of our staff and yours are taking a well-deserved break. We also want to avoid any disruptions or incidents that could affect your business operations or customer satisfaction.

What do you need to do?

If you have any planned changes that need to be implemented before or after the change freeze period, please submit them to our Service Desk as soon as possible. We will review them and schedule them accordingly. If you have any urgent changes that need to be done during the change freeze period, please contact our Service Desk and we will assess them on a case-by-case basis.

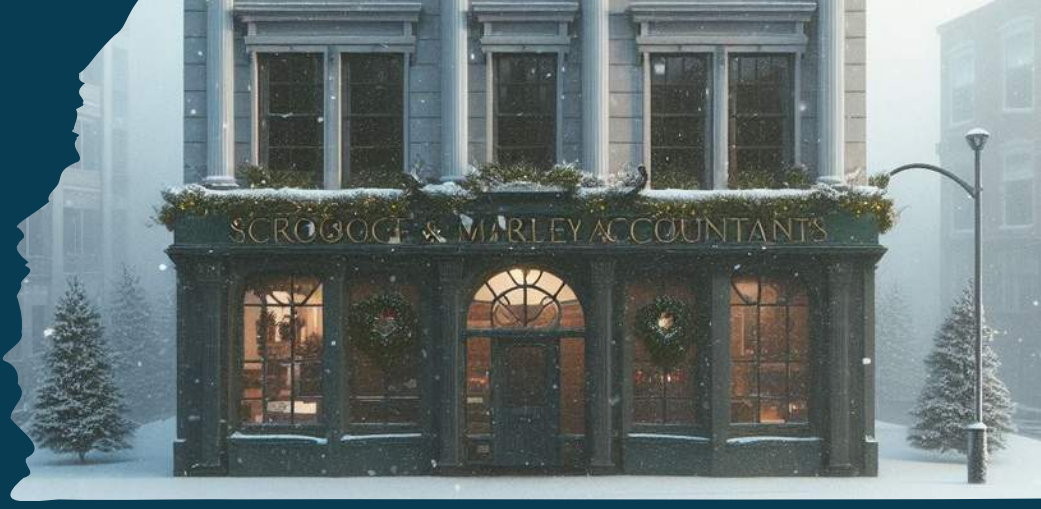
For telephony customers: if you require assistance with call diverts or seasonal voicemail greetings (e.g. changes to opening hours) please let us know by Monday 18th December to ensure that we have ample time to action your request. We can't guarantee the completion of requests received after this date.

We appreciate your cooperation and understanding in this matter.

For further information, please contact your account manager or a member of the Service Desk.

A Cyber Christmas Carol

How Three Technology Solutions Saved Christmas



Ebenezer Scrooge was a successful but miserly business owner who ran a large accounting firm. He hated spending money on anything that he considered unnecessary, especially technology and cybersecurity. Ebenezer still used outdated software, hardware, and practices that put his business at risk of cyberattacks and data breaches. He thought that cybersecurity was a waste of time and money and that he could handle any problems by himself.

One night, on Christmas Eve, Scrooge was visited by the ghost of his former partner, Jacob Marley, who warned him that he would face a terrible fate if he did not change his miserly ways. Marley warned Scrooge that he would be visited by three technology solutions, each representing a different aspect of cybersecurity: past, present, and future. They would show him the error of his ways and the consequences of his actions.

The Ghost of Cybersecurity Past transported Scrooge back to the early days of his business when he was a young and ambitious entrepreneur. It showed him how he used to invest in the latest technology and security solutions, and how they helped him grow his business and gain a competitive edge. The spirit also showed him how he gradually became greedier and stingier and started to neglect his cybersecurity needs. The ghost reminded him of the incidents that he suffered as a result, such as malware infections, ransomware attacks, phishing scams, and identity theft. The spirit explained to Scrooge that he could have avoided these problems if he had kept his technology and security up to date and followed cybersecurity best practices.

Next appeared the Ghost of Cybersecurity Present, who showed Scrooge the current state of his business, and how vulnerable it was to cyber threats. It revealed to him the hidden costs of his poor cybersecurity, such as lost productivity, reputation damage, legal liability, the high price of insurance coverage, and customer displeasure. The ghost also showed Scrooge the benefits to his competitors, who had invested in modern technology and security solutions, and how they were able to offer better services, attract more customers, and generate more revenue. The kindly spirit showed Scrooge that through his shortsightedness he was losing his competitive advantage and risking his business, and that he needed to improve his cybersecurity posture as soon as possible.

The Ghost of Cybersecurity Future was the most fearsome and terrible apparition. The spirit showed Scrooge a bleak vision of what would become of his business if he did not change his ways. It showed him a catastrophic cyberattack that compromised his entire network, destroyed his data, and exposed his confidential information. The spirit also revealed the devastating consequences of the attack, such as a costly lawsuit, audits, investigations, regulatory fines and, ultimately, bankruptcy. The ghost showed him the impact of the attack on his employees, customers, partners, and suppliers, and how they suffered from emotional distress and financial losses. Finally, the spirit showed Scrooge the inevitable outcome of his negligence and ignorance, and that he had no one to blame but himself.

When, on Christmas morning, Scrooge awoke from his nightmare and realized that he had been given a chance to change his fate. He decided to act immediately and invest in the technology and security solutions that he needed to protect his business. He updated his software and hardware, implemented a comprehensive cybersecurity strategy, and educated his employees and customers on cybersecurity awareness. He also became more generous and caring and started to share his wealth and knowledge with others. He transformed his business into a secure, successful, and sustainable enterprise, and enjoyed the benefits of cybersecurity.

Scrooge learned how to appreciate the spirit of Christmas, and faithfully promised to live in the Past, Present and Future of cybersecurity. He even sent his long-suffering, underpaid clerk, Bob Cratchit, on a National Cyber Security Centre (NCSC) advanced training course, giving him an above-inflation salary increase. And so, as Tiny Tim from IT support said, ‘A Merry Christmas to us all; God bless us, everyone!’

If you would like to know more about improving the cybersecurity of your business without the intervention of the spirit world, then please contact Modern Networks today.

Embrace the Future: Technology Trends to Shape 2024

As we approach the end of 2023 and the dawn of 2024, the landscape of technology is rapidly changing. Today, UK businesses are presented with numerous opportunities to enhance their operations, streamline processes, and gain a competitive edge. Let's explore the key technology trends that are expected to make a significant impact on UK businesses in the coming year.

Artificial Intelligence (AI) and Machine Learning (ML) – The Power of Automation and Insight

AI and ML are transforming the way businesses operate, providing the ability to automate tasks, improve decision-making, and gain deeper insights from vast amounts of data. From customer service chatbots to fraud detection systems, AI is revolutionising industries. Businesses that embrace AI and ML will be well-positioned to enhance efficiency, reduce costs, and deliver personalised customer experiences.

5G – Unleash the Potential of Next-Generation Connectivity

5G networks are set to revolutionise the way businesses connect, offering lightning-fast speeds, lower latency, and increased capacity. This will open new possibilities for applications such as augmented reality (AR), virtual reality (VR), and the Internet of Things (IoT). Businesses can expect to see enhanced productivity, improved collaboration, and new revenue streams as 5G becomes more widely available.

Cybersecurity – Safeguarding the Digital Workplace in an Evolving Threat Landscape

In today's digital world, cyberattacks are becoming more sophisticated, which makes cybersecurity a top priority for businesses, regardless of their size. To protect sensitive information and prevent cyber threats, it's crucial to invest in strong security solutions and implement comprehensive data protection measures. Furthermore, educating employees about cybersecurity best practices is an essential step to ensure that everyone in the organization is aware of potential risks and how to avoid them.

Cloud Computing – Embracing Scalability, Flexibility, and Cost-Efficiency

Cloud computing has become a cornerstone of modern business operations, providing businesses with access to scalable, flexible, and cost-efficient IT infrastructure. By migrating workloads to the cloud, businesses can reduce upfront hardware costs, enhance agility, and focus on their core business objectives.

Data Analytics – Turning Data into Actionable Insights

Data is the lifeblood of modern businesses, and data analytics is the key to unlocking its value.

By harnessing the power of data analytics, businesses can gain insights into customer behaviours, optimize operations, identify new market opportunities, and make informed decisions that drive growth. Launched in May 2023, Microsoft Fabric, for example, enables businesses to harness data analytics and AI to improve everyday workplace operations.

Sector-Specific Trends – Harnessing Technology for Industry-Specific Innovations

In addition to these general trends, there are also several sector-specific trends that are worth watching. For instance, the retail sector is embracing AI and ML to personalise customer experiences and optimize pricing, while the healthcare sector is using technology to deliver more personalised and effective care. The financial sector is leveraging technology to improve risk management and compliance.

Real-World Examples of Technology Innovation in UK Businesses

UK businesses are already embracing technology to innovate and improve their operations. Here are a few examples:

- British Land is using cloud computing to store and manage its data securely while making collaboration across its teams easier.
- Barclays is using AI to detect fraud and prevent financial crimes.
- Sainsbury's is using AI to optimize its supply chain and reduce food waste.
- AstraZeneca is using AI to accelerate drug discovery and development.
- Ocado is using AI to help automate its warehouses and improve its delivery service.
- Aviva, one of the UK's largest insurance companies is using cloud computing to improve the efficiency of its operations, reduce costs and improve customer services.

Embracing Technology for a Brighter Future

In today's fast-paced world, technology is constantly evolving and businesses that keep up with the latest trends and innovations are more likely to succeed. Investing in emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), 5G, cloud computing, cybersecurity, and data analytics can help UK businesses increase efficiency, improve customer experiences, and stay ahead of the competition. As we look towards the future, embracing technology will be essential for UK businesses to thrive and navigate the rapidly changing digital landscape in the years to come.

To learn more about how technology can help your business achieve its goals this coming year, contact Modern Networks today.

It’s time to turn the tide on phishing attacks

Phishing attacks have reached record highs this year. Worryingly, in the third quarter of this year alone, **phishing attacks skyrocketed by a staggering 173%**, compared to the previous three months.

And malware? It’s not far behind, with a 110% increase over the same period.

Let’s put this into perspective. Imagine you’re on a quiet beach, enjoying the sun and the surf. Suddenly, the tide starts to rise rapidly. Before you know it, your picnic basket is floating away, and you’re knee-deep in water. That’s what’s happening in the cyber world right now.

According to a report, the ‘phisherfolk’ group were most active in August, casting out more than 207.3 million phishing emails. That’s nearly double the amount in July. September wasn’t much better, with 172.6 million phishing emails.

But who are these cyber criminals targeting? Old favourites Facebook and Microsoft continue to top the charts, with Facebook accounting for more phishing URLs than the next seven most spoofed brands combined.

So, what’s the bottom line here?

Your business could be next.

Phishing attacks are like a rising tide, and if you’re not careful, they can quickly sink your business. They target everyone - from tech giants to financial institutions, and even government agencies. The question is - are you prepared?

Take a moment to consider the authenticity of emails. Are they from a trusted source? Do they contain suspicious links? Are they asking for sensitive information?

Make sure your employees are aware of the risks. Encourage them to think twice before clicking on a link or downloading an attachment. After all, a moment’s hesitation could save your business from a devastating cyber-attack.

And don’t forget about integrated email security solutions and phishing awareness training. They could be the the thing that best helps you prevent an attack.

So, as the tide of phishing attacks continues to rise, remember – it’s better to be safe than sorry. If you need any further help or advice, get in touch.

CHRISTMAS TREE TRIVIA

Did you know that the world’s first artificial Christmas tree was made of goose feathers dyed green? It was invented in 19th century Germany as a response to the deforestation caused by the demand for natural trees. The feather trees were popular until the 1930s when they were replaced by more realistic-looking trees made of brush bristles. These were the ancestors of the modern artificial trees.

Q: If I accidentally close a tab in Chrome, is there an easier way to get it back than searching it up again?

A: Yes, you can bring back the closed tab with a simple keyboard shortcut. If you’re using Windows, ChromeOS or Linux it’s CTRL+Shift+T; for Mac it’s CMD+Shift+T.

Q: I’m finding ChatGPT is not giving me great answers and is inaccurate – what am I doing wrong?

A: You’re probably not being specific enough with your question. Also check your question for typos and slang… too many and you won’t get great responses.

Q: I’m fed up having to minimise my windows when I want to look at my desktop – surely there’s an easier way?

A: If you’re using Windows, there is! Look all the way to the bottom and right, beyond the date and time and you’ll find a little sliver of a secret button. Click it to minimise all your open windows at once, then click it again to bring everything back.

This is how you can get in touch with us:
CALL: 01462 426500 | EMAIL: info@modern-networks.co.uk
WEBSITE: www.modern-networks.co.uk

modernnetworks