Meeting The Cyber Security Challenge

Managing Cyber Risk for IT Managers and Directors

YOUR IT DEPARTMENT

Introduction

Cyber crime is nothing new, the origins of cyber crime can be traced back to 1834. Attackers stole financial market information by accessing the French telegraph system. From that moment on, cybercrime has grown exponentially, marked by an intriguing evolution of tactics, techniques, and procedures — all implemented for malicious gain.

Today, IT Managers and IT Directors face a multitude of challenges when it comes to cyber security.

For most there is simply not enough time and resources to tackle those challenges alone. Due to this the attitude to working with outsourced IT has changed.

Once viewed as a competitor or threat to the IT Manager or inhouse team, many have found that partnering with a Managed Service Provider (MSP) can be a game-changer for IT Managers and IT Directors.

In this eBook we look at 10 of the major challenges facing IT Managers and IT Directors around cyber security and how working in partnership with an MSP can help address those challenges.

The Challenges

Rapidly Evolving Threat Landscape:

Cyber threats are constantly evolving, with hackers and malicious actors employing sophisticated tactics to exploit vulnerabilities. New attack vectors emerge regularly, making it challenging for IT managers and directors to stay ahead and effectively protect their organisation's digital assets.

MSPs possess specialised threat intelligence and proactive monitoring capabilities, allowing organisations to stay ahead of sophisticated bad actors and effectively protect their valuable digital assets from emerging attack vectors.

Resource Constraints:

IT departments often face limited budgets, time, and personnel. Allocating resources for cyber security initiatives can be difficult, especially when competing with other IT projects and operational priorities. Striking the right balance between cyber defence and other IT responsibilities is a constant challenge.

By leveraging the expertise of MSPs, organisations can optimise resource allocation for cyber security initiatives without compromising other essential IT projects and operational priorities. This collaboration enables IT leaders to strike an optimal balance between cyber defence and core IT responsibilities.

Cybersecurity Talent Shortage:

The demand for skilled cyber security professionals far exceeds the available talent pool. Finding, hiring, and retaining qualified experts can be a significant challenge for IT managers and directors, leading to potential skill gaps in their security teams.

MSPs offer a practical solution by augmenting internal teams with their pool of qualified experts. This access to a diverse talent pool allows organisations to bridge skill gaps and enhance their overall cyber security capabilities, ensuring robust protection against cyber threats.

Balancing Usability and Security:

Striking the right balance between user experience and security is essential. Implementing stringent security measures might hinder productivity and user convenience, while lenient measures can expose the organisation to vulnerabilities. Finding the right balance is a constant challenge.

MSPs excel at implementing tailored security measures that do not impede usability. Their expertise ensures a user-friendly yet fortified security environment, enhancing both productivity and protection.

Complex IT Infrastructure:

Many organisations operate in intricate and interconnected IT environments, including cloud services, third-party integrations, and legacy systems. Securing these diverse components while ensuring seamless functionality is a complex task, requiring careful coordination and robust security measures.

MSPs, well-versed in securing diverse infrastructures, provide expert guidance to safeguard every component of the IT landscape.

Compliance and Regulatory Requirements:

Organisations must adhere to various industry regulations and data protection laws. Meeting these compliance requirements while maintaining effective cyber security practices requires meticulous planning and ongoing monitoring.

MSPs serve as invaluable partners in navigating this intricate regulatory landscape. Their meticulous planning and ongoing monitoring ensure that organisations meet compliance requirements while maintaining robust cyber security practices.

Insider Threats:

Insider threats, whether unintentional or malicious, pose a significant risk to organisations. Balancing trust in employees while safeguarding against potential insider attacks can be a delicate challenge.

MSPs collaborate with internal teams to implement comprehensive security policies and access controls. Through continuous monitoring and risk assessment, MSPs contribute to a well-balanced strategy that addresses insider risks while maintaining a trusting work environment.

Third-Party Risk Management:

Organisations often collaborate with external vendors and partners, increasing the risk of cyber threats through supply chain attacks or data breaches. IT managers and directors must diligently assess and manage third-party cyber security risks.

Your MSP can conduct thorough assessments to evaluate third-party cyber security risks. This empowers organisations to engage with external collaborators confidently, protected against potential security vulnerabilities.

Lack of Cybersecurity Awareness:

Despite advancements in cyber security education, employee awareness remains a critical challenge. Human error, such as falling victim to phishing scams, can still be a major factor in security breaches.

MSPs bolster cyber education efforts with security awareness training. They conduct simulated phishing exercises and can provide interactive workshops, empowering employees to recognise and mitigate cyber risks effectively.

Convincing Decision Makers:

Communicating the importance of investing in cyber security as a strategic business enabler can be difficult. Convincing top-level executives and decision makers that cyber security solutions are investments, not just costs, requires effective communication and data-driven business cases.

MSPs equip IT Managers and Directors with comprehensive reports and insights that demonstrate the value of cyber solutions. With MSPs as strategic partners, organisations can secure top-level executive buy-in for cyber security investments.

Getting Started with an independent risk assessment.

An external cyber risk assessment can be highly beneficial for an IT Manager or IT Director and a great way to start working with an MSP.

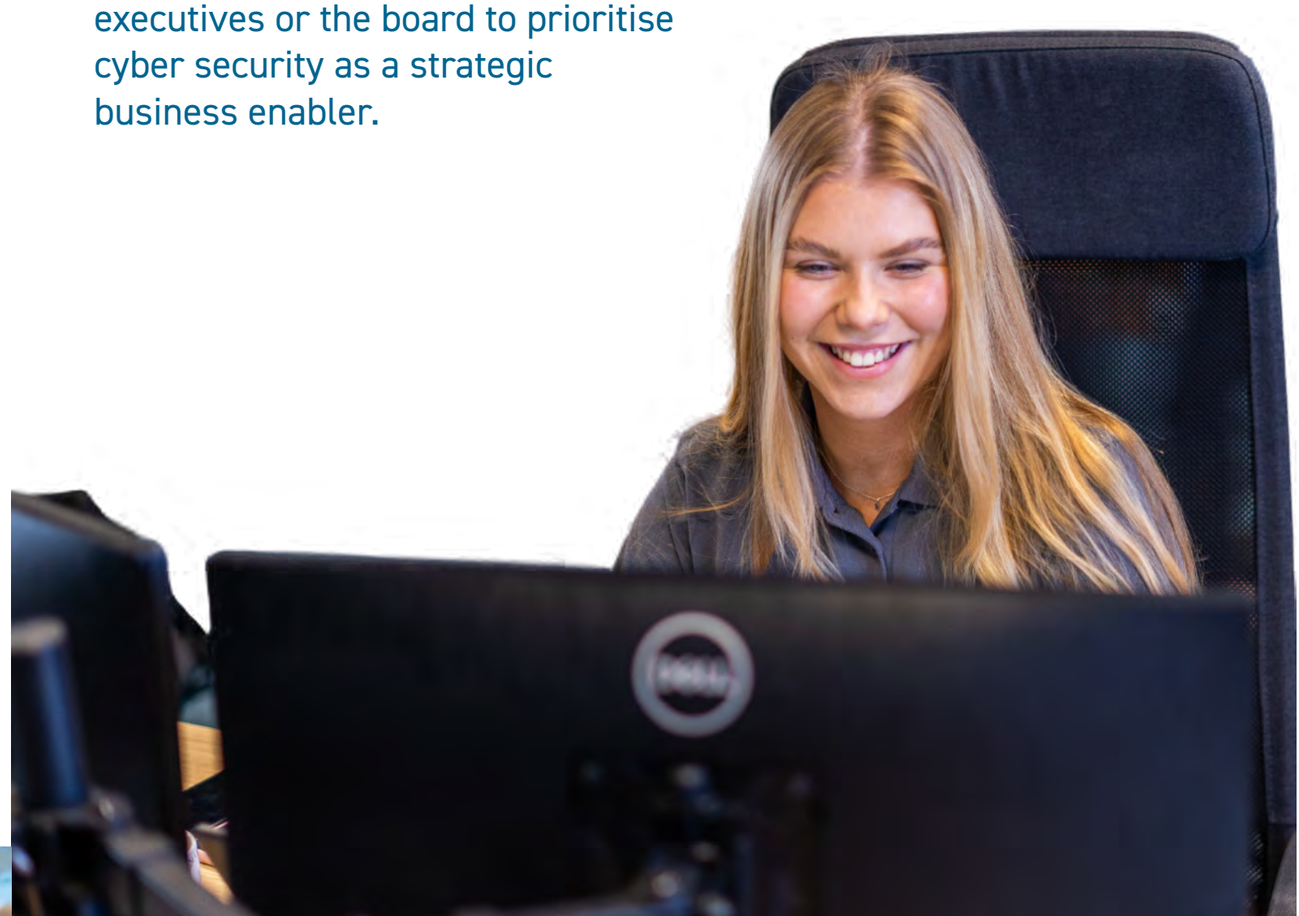
An external assessment provides an independent and objective evaluation of your cyber security posture. External assessments are conducted by impartial experts with a fresh perspective. This allows for a comprehensive and unbiased view of potential vulnerabilities and risks. This is not about pointing out 'mistakes' – it's about looking at risks and how they can be mitigated.

Cyber security is a complex and rapidly evolving field, and MSP's possess in-depth knowledge and experience in identifying and mitigating various cyber threats. Their skills in using cutting-edge tools and methodologies enable them to uncover hidden vulnerabilities that might have gone unnoticed otherwise. This comprehensive insight empowers IT Managers and Directors to make informed decisions about strengthening their organisation's cyber defences.

Furthermore, an external assessment enhances an organisation's overall cyber resilience. By identifying weaknesses and gaps in existing security measures, IT leaders can proactively address potential threats before they escalate into full-blown security incidents. Implementing the recommendations from an external assessment bolsters the organisation's ability to detect, prevent, and respond to cyber attacks effectively.

Finally, an external cyber risk assessment can also serve as a powerful communication tool for IT Managers and Directors. The findings and recommendations from the assessment provide tangible evidence to stakeholders and decision makers about the importance of cyber security investment.

The report can be used to build a compelling business case for allocating resources, budget, and support towards cyber security initiatives, especially when convincing top-level executives or the board to prioritise cyber security as a strategic business enabler.



Ready to Partner Up?

Book a cyber security assessment

About Us

Your IT are one of the UK's leading Managed Service Providers. We provide managed services to over 100 businesses and 2500 end users in the Midlands, Yorkshire and across the UK.

We have developed our cyber security offering over the past 5 years, training staff and developing our UNIFIED cyber security solution into what we believe is one of the most comprehensive solutions on the market.

Featuring Next Gen AV, DNS Filtering, EDR, Email threat protection and fraud prevention and 24/7 XDR backed SOC plus much more linked to a full service desk, with incident response and remediation.

With a number of additional services available such as Security Awareness training, UNIFIED can be tailored to your needs.

Your IT Department

Unit 8 Farrington Way
Eastwood
Nottingham
Nottinghamshire
NG16 3BF

T: 0115 822 0200
E: info@your-itdepartment.co.uk
W: your-itdepartment.co.uk

Follow us on social media: