LANTECH
MANAGED IT SUPPORT, SECURITY & CLOUD

September 2023

THE DOWNLOAD

As September unfolds, ushering in the latter half of the year, we pause to reflect and share our journey's progress with you.

2023 has been a truly remarkable chapter, seeing our valued customers thrive across diverse industries. In January, our dedication to delivering an exceptional customer experience earned us the prestigious "Customer Experience Champion of the Year" award from Superops. This accolade reinforces our unwavering commitment to placing you, our customers, at the heart of all we do.

In February, we achieved a significant milestone, with over a quarter of our team members now remarkable women in the tech sphere. March brought us the celebration of a momentous 15-year partnership with Leinster Rugby— a collaboration steeped in shared values of teamwork, resilience, and innovation. Our IT expertise has been a steadfast support, contributing to their incredible journey.

Our recognition as "IT Support Company of the Year" at the CIO/CTO Awards in June was a testament to the unwavering dedication of our team, consistently exceeding expectations to provide top-tier IT support to our clients.

And now, an exciting new chapter unfolds: we are thrilled to announce our presence in the UK. Our expansion marks an important stride as we extend our reach to serve our clients on an international scale.

Thank you for being an integral part of the Lantech family.

Peter Strahan

CEO, Lantech IT Services

CONTENTS

THE CIO & IT AWARDS 2023

CIO & IT LEADERS AWARDS 2023

LANTECH
MANAGED IT SUPPORT, SECURITY & CLOUD

WINNER

IT SUPPORT COMPANY OF THE YEAR

WE WERE DELIGHTED TO WIN THE IT SUPPORT COMPANY OF THE YEAR AT THE CIO & IT AWARDS 2023.

'Recognising achievement in technology innovation and leadership in Ireland.'

This prestigious black-tie gala awards ceremony celebrated the change makers and disruptors that are taking their organisations to new heights with their approach to IT strategy.

In what has been a turbulent yet exciting year for many CIO's and IT Leaders, there was no better time to reflect on our achievements and give recognition to those who have not only led their organisation through challenging times in the wake of the pandemic, but took the opportunity to achieve radical digital transformation within their organisation to become market leaders and realise true business value.

Thanks again to all our hardworking team, customers and suppliers.

UNDERSTANDING MICROSOFT SECURE SCORE: A COMPREHENSIVE GUIDE FOR BUSINESSES BY LANTECH

Do you know your score?

As a managed service provider (MSP), we understand that businesses face an ever-evolving landscape of cyber threats. That's why it's crucial for organisations of all sizes to be aware of their security posture. One valuable metric that can help you gauge your company's cybersecurity is the Microsoft Secure Score. In this short article, we'll introduce you to the concept of Microsoft Secure Score, explain its importance, and discuss how partnering with our team of experts can help you protect your business. Let's get started!

What Is Microsoft Secure Score?

Microsoft Secure Score is a numerical representation of your organisation's cybersecurity posture. The score ranges from 0 to 100, with higher scores indicating better security. It provides insights into the security measures you have in place and offers recommendations for improvement. The score is based on various factors, such as the implementation of multi-factor authentication (MFA), policies, and basic settings being implemented.

Why Is Microsoft Secure Score Important?

Your Microsoft Secure Score is vital because it helps you understand the current state of your cybersecurity and identifies areas for improvement. Here's a general guideline to interpret your score:

Below 30: Serious concern –
Immediate attention required

Below 50: Significant risk –
High priority improvements needed

Below 70: Requires review –
Examine further improvements that can be made in the M365 tenant

Keep in mind that your target score should be based on your unique security risks and requirements. It's essential to assess your organisation's specific needs and work towards a higher score to protect your business from potential cyber threats.

UNDERSTANDING MICROSOFT SECURE SCORE: A COMPREHENSIVE GUIDE FOR BUSINESSES BY LANTECH

How to Improve Your Microsoft Secure Score?

Improving your Microsoft Secure Score is all about implementing recommended security measures and best practices. As a specialist IT Services Provider, we can help you take the following steps:

- **Assess your current score:** We'll help you access your score in the Microsoft 365 Security Center and analyse your organisation's security status.
- **Prioritise recommendations:** We'll identify the most critical security issues and help you tackle them first to have the most significant impact on your overall score.
- **Implement and enforce multi-factor authentication (MFA):** We'll enable and enforce MFA for all users, providing an additional layer of security for account access.
- **Educate your employees:** We'll train your staff on cybersecurity best practices, including recognising and reporting phishing attempts, to reduce the risk of human error.
- **Keep systems up-to-date:** We'll ensure that all software and systems are updated with the latest security patches.

Partner with Lantech for a Higher Secure Score

By partnering with our team of cybersecurity experts, you can expect:

1. Comprehensive security assessment: We'll evaluate your current security posture and provide customized recommendations for improvement.
2. Best practices implementation: Our experts will work with your team to implement necessary changes to boost your Secure Score.
3. Continuous monitoring and support: We'll monitor your security environment to ensure ongoing improvement and provide support when needed.
4. Employee education and training: We'll deliver tailored cybersecurity training to help your employees become security-aware and proactive.

Understanding your Microsoft Secure Score is crucial for maintaining a strong cybersecurity posture.

By knowing what it is, recognising its importance, and partnering with a trusted MSP like Lantech, you can protect your business from the ever-evolving landscape of cyber threats.

Don't wait, ask your IT provider what your secure score is and start improving your Microsoft Secure Score today

WE LOST: THE UNSEEN POWER OF DEFEAT

They say the toughest lessons are learnt in defeat. Last month, this was exemplified by the players we proudly support - Leinster Rugby. A bitter pill to swallow, one point short of victory, they demonstrated the true meaning of resilience, of unity, of team spirit.

Retreat could have been the natural instinct, to isolate and mull over every decision leading to that moment, no doubt there will be many lines written in the papers. But in the face of defeat, they stuck together and at a post-match event they came together when the easier decision may have been to disappear. Why? Because being together amidst failure is the loudest testament to the unshakeable belief in their collective potential.

The mantra of the night was “we go again.” This simple, yet powerful phrase spoke volumes of their resilience, their indomitable will to bounce back stronger, better, faster.

Last month’s loss unveiled a fundamental truth - a true team stands together in defeat as they would in victory. Their strength is derived not just from their wins, but from their losses too. Forged from triumphs and trials, Leinster Rugby is more than just a team; they’re a testament to unity and resilience.

It’s often said that in business, as in sport, you learn, you evolve, and you strive for greatness. The setbacks we face, the losses we endure, they’re stepping stones to a future that’s brighter, stronger. As Leinster Rugby showed us, they are opportunities to learn, to grow, and to become the best version of ourselves.

The players might have been dejected, but by the end of the night, they had turned the event into a celebration of the season’s end. Their determination to “go again” was evident. In the face of defeat, they stood together, showcasing the remarkable culture they’ve nurtured.

So yes, they lost. But they also gained - insights, experience, strength. Strength to “go again”, to face any challenge that comes their way. The resilience displayed by Leinster Rugby is not just inspirational for sports fans, but a powerful lesson for businesses too.

In our journey, as in theirs, we rise and fall together. Today, they rise from defeat, more focused, more determined, ready to write their next chapter. Because they are a team, in victory and in defeat.

We Go Again.....

SMALL BUSINESSES ARE TAKING A BIG CYBER SECURITY RISK

There's something very worrying about the way SMEs are approaching their cybersecurity. Whilst recognising that it should be a high priority, they don't prioritise putting adequate defences in place.

It's easy to blame other pressures. The economic climate is undoubtedly tough with high energy prices, skills shortages and input costs soaring. And these factors are perhaps easier to address. They don't require specialist IT knowledge. And unlike the nebulous threat of a potential cyber-attack, results can be quickly realised and easily quantified.

But sometimes SMEs aren't even aware they're at risk. They have an IT provider or in-house team and assume that they are being protected. Their lack of knowledge, or lack of engagement with the technical language, or even a surfeit of trust, can leave them exposed. It's unthinkable that an organisation wouldn't have an independent audit of its accounts and financial procedures, but few organisations think about scrutinising their IT provision.

We have to ask why because every cybercriminal knows that this is happening. They know which types of organisations are vulnerable and why. Cyber-attacks on big corporations make the big headlines, but being a smaller organisation doesn't make you safe. Without robust defences, any organisation is an easy target.

The SME deciding to face up to these threats and take steps to defend itself will find plenty of advice online. They will discover warnings about the increased risks due to hybrid working practices. They will find out about the problems arising with the use of multiple devices, apps, smartphones and the like. They will perhaps learn about the risks of plugging a USB storage device into their company laptop. And to mitigate the threat they may implement various policies or have an in-house awareness campaign.

All that's helpful, but it's not the answer. You can't cherry-pick certain risks, tackle them once and assume that going forward they're dealt with. New threats emerge constantly. What's more, personnel change. Employees forget they're logging in from a Wi-Fi hotspot. They don't spot the hijacked email thread, or they share the odd password so that a colleague can get on with the job. One-off solutions aren't enough. You need an ongoing cybersecurity strategy that's continually reviewed, adequately resourced and well-managed.

And yes, that will have a cost. But the cost will be nothing compared to the cost of a ransomware attack or the reputational damage of a serious data breach.

Get the board together.
Talk about this issue and do it now.

1. ***Find out about Cyber Essentials.*** It's a great place to start boosting your understanding of cybersecurity and offers a structured way to mitigate risk.
2. ***Ask your IT provider*** – or your in-house team – what cybersecurity measures are in place to protect your operation and how they link to international standards. Be prepared for a serious rethink if their answers are vague or evasive.
3. ***Build a strategy around cyber security*** and how your business uses and will use technology.

We understand the pressures of running a business – we live it every day, too – but with cyber threats, you can't afford to take the risk. Learn about the threats. Develop a strategic and ongoing approach to preventing attacks. Doing so will give you much more peace of mind than you'll ever find by burying your head in the sand.

If you'd to chat about the issues raised or would like our help, just call.

YOU GET A REQUEST IN AN EMAIL... DO YOU ACTION IT?

I guess if you're asked to transfer your life savings to someone you've never heard of, you'll know it's a scam. But what if everything looks okay? What if it seems to be from someone you know, chasing up an action, or requesting payment for work that's been done? That's got to be okay, hasn't it?

Well, unfortunately, no. More and more hackers are breaking into email threads and pretending to be the original participant. You were exchanging legitimate messages with Fred, but now you're corresponding with a cybercriminal who has snaffled enough information – names, logos and other details – to make his request seem legitimate.

It's a smart trick because it's not easy to spot. And, unfortunately, it's increasingly common. Reported cases of email thread hijacking doubled in the last twelve months. And the attacks come in different guises. If they don't include a payment request, don't assume you're safe. Click a link in one of these messages and you could unleash malicious software without even being aware. You could accept an invitation and disclose personal information that puts you at risk.

This is a real threat. Even if you're aware of the email hijacking trend, in the busy day-to-day routines of work life, it's easy to trust the messages that drop into your inbox. It's even easier to be fooled when you're already in the midst of an email conversation.

We urge you to treat everything with caution, scrutinise details, and don't assume that because you know the name of the apparent sender that the message is genuine.

What can you do to protect your business?

1. Implement the basics: like removing local admin rights from all computers (take our 15 step checklist and see how many of the basics you have enabled)
2. Have robust accounting processes: for example PO number, approval policy, double verification for payments and bank detail updates etc.
3. Ensure your staff are up to date with cyber security with a simple and regular training program
4. Speak to your provider or give us a call, it doesn't cost a penny to have a chat.

TAKE A BREAK – EVEN IF IT'S A BUSY ONE

I believe that even CEO's need to find time for personal and professional growth, but it's not easy. There's always a stack of things to do, all of which can seem like the most pressing or important. When the idea of travelling to a conference comes up, it can seem like the proverbial straw on the camel's back.

Guess what – when you're busy, a break from the routine, investing some time in yourself can prove just what's needed.

Earlier this year, Lantech had the pleasure of being invited and hosted by Nerdio at their conference Nerdiocon23, a fantastic experience. I spent time with like-minded individuals, shared stories about the challenges we're all facing, had a laugh, discovered new innovations, was inspired and energised, Spending time with the Nerdio team and Joseph Landes was very informative and allowed us to reaffirm our long-term strategy

When you're busy it's too easy to hunker down, doing the work, ignoring everything beyond your current priority. Being around other leaders provided a reminder of the close community that exists in the technology sector. It was busy, hectic even, but in many ways, it was precisely what I needed.

The conference was technical, which suited our CTO Daniel Cronin, but I'd gleaned far more than tech knowhow. Sitting here in the airport while I write this waiting for our flight to be called I'm thinking about all the notes taken, conversations had and the little nuggets of information consumed. There were so many takeaways from the conference, I want them

all captured, particularly those concerning strategy. I have a new perspective and a sense of clarity on where we're going and the value we offer.

Getting time away from the desk allowed me to refocus on what's important. As someone who's always on the go, and rarely gets enough sleep, it gave me the chance for a reset. For a few days, I prioritised my wellbeing, and I slept like a log.

The to-do list won't have shrunk while I was away and it's right back into a busy schedule, but I'm energised and excited about the work. We're delivering benefits to our clients that help them stay secure, productive and profitable. What could be better?

Without a shadow of doubt, the trip worked wonders. I'm restored, refreshed and ready to serve.

Peter Strahan - CEO

THIS IS REAL GROWTH

An 2022 we added resources in engineering, sales and Account Management, In 2023 we have so far added 4 and we're recruiting for an additional 4 with 3 hopefully being filled this week, looking forward we have no let-up in recruitment.

We're seeing a significant increase in demand as businesses look to leverage technology as part of their strategy, become more efficient, embrace secure and productive remote and hybrid working. Cyber Security while critical still seems to be lagging in businesses, however awareness is growing, it is just unfortunate it takes some level of incident to spur them into action.

While the Digital Transformation phase has been around for some time, it's only since late 2022 and in 2023 we're seeing businesses embrace technology fully. Most businesses don't know where to begin which shows a lack of available talent in the market. We're certainly seeing that when strategic consulting services are coupled with the technical execution there is a high rate of adoption. With all the new and improved platforms such as Azure and M365, education around technology adoption has become a key critical growth area for service providers.

YOU SHOULD CHOOSE AN MSP WITH MICROSOFT'S "SOLUTION PROVIDER" ACCREDITATION. HERE'S WHY.

The world of work has changed. The mass move to remote working triggered by the coronavirus pandemic hasn't reversed.

More and more people, businesses and other organisations are choosing a hybrid working model. They are discovering enhanced productivity, more enjoyment and new ways to collaborate – even across huge distances. It's been called the modern way of working and has led to the creation by Microsoft of a new accreditation – the Modern Work Solution Provider – which reflects the change, the challenges and the opportunities it presents.

But some MSP's haven't embraced that change or pursued the accreditation. As a consequence, they can't adequately support their clients in this new diverse but powerful working environment. Their clients are unable to capitalise on potential productivity gains and often experience frustration when systems that should link seamlessly don't, or when their data is exposed in a security breach. Often the benefits that cloud-based systems can deliver, don't materialise. Applications don't connect, cybersecurity is poor, there's little thought given to the spiralling costs of multiple software licences.

At Lantech, we're proud to have been granted this new Microsoft accreditation. It's part of Microsoft's Cloud Partner Program and supports our proactive approach to the promotion of safe and secure hybrid working practices. For a client wishing to transform their operation with cloud-based digital solutions, the award demonstrates our team's expertise and commitment.

I'm Peter Strahan, Lantech's CEO, and frankly, I believe the lax approach of some MSPs is irresponsible. Clients rely on the advice, support and 'expertise' of their IT provider, but if it's not up to scratch, in this new world of work, the client won't thrive. As technology advances the relevance of certain accreditations is diminishing – Microsoft's Silver and Gold accreditations have now been retired – and I believe that accreditations must always reflect the evolving nature of how we work.

An accredited partner will help users get the best from technologies like Microsoft 365, but the new accreditation isn't easy to achieve. Standards are high and the work is demanding, but it's worthwhile. To deliver the best possible service, we have to have the best possible knowledge and understanding.

We're well on the way to a second new accreditation. In the next few weeks, we expect to become an accredited Azure Infrastructure Solution Provider. Too many organisations use unverified providers for Azure work, but I urge them to think carefully about their choices. We hear about fast-changing technology all the time, and it has become something of a cliché, but it is true. These developer accreditations really are the simplest way of deciding whether your provider has the skills and knowhow needed to enhance your performance and keep you safe.

The key takeaway: if success matters to you, look closely at your provider's accreditations.

LANTECH IN THE COMMUNITY

We are thrilled to announce our sponsorship of the Ashbrook Open (a local tennis club) and the U10's Beachwood football teams for the upcoming 2023/2024 season.

As a firm believer in the power of sports in nurturing talent, promoting teamwork, and fostering community spirit, we are proud to support these young athletes in their pursuit of excellence. By providing financial assistance, equipment, and resources, we aim to contribute to the growth and development of both clubs. We are excited to witness the achievements and successes of these talented tennis players and football enthusiasts as they work towards their goals. Our sponsorship is a testament to our commitment to promoting a healthy and active lifestyle among the youth, and we look forward to a successful and rewarding season for both teams.

Join us in cheering for Dan and Peter as they take on the Chicago Marathon, pushing their limits to make a difference.

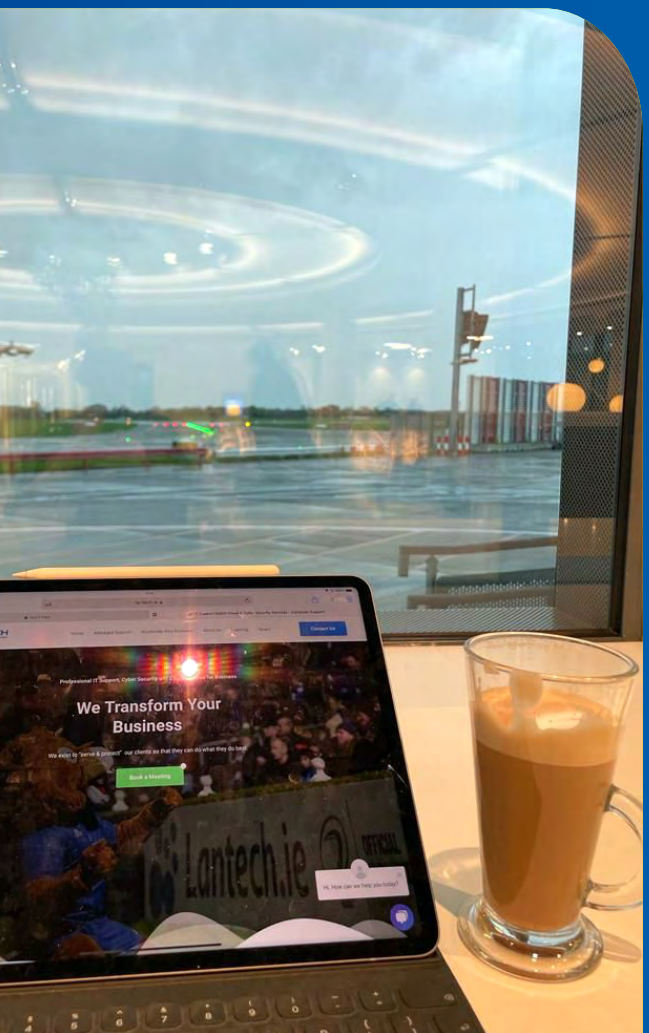
Let's rally behind them and dig deep to support their noble cause for charity.

Watch out for the donation link on their LinkedIn profiles soon.

BANK OF AMERICA
Chicago Marathon

CHECKLIST: 15 ESSENTIAL STEPS TO PROTECT YOUR BUSINESS FROM A CYBER ATTACK.

Email hello@lantech.ie for your copy.



HAVE A QUESTION ABOUT TECHNOLOGY IN YOUR BUSINESS?

Drop us a DM to organise a coffee, it's on us.

LANTECH
MANAGED IT SUPPORT, SECURITY & CLOUD

+ 353 1 4760030

hello@lantech.ie

www.lantech.ie