JANUARY / FEBRUARY 2024

BITS & BYTES

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE:

We love technology and we love helping people.

Give me a call today for a quick (non-salesy) chat to find out whether my team and I can help you better secure your data and get more out of your existing technology!

- **Lee Hewson**
Founder and MD

HOW TO ORGANISE YOUR CYBERSECURITY STRATEGY INTO LEFT AND RIGHT OF BOOM

In the pulsating digital landscape, every click and keystroke echoes through cyberspace. The battle for data security rages on. Businesses stand as both guardians and targets. Unseen adversaries covet their digital assets.

Businesses must arm themselves with a sophisticated arsenal of cybersecurity strategies. On one side, the vigilant guards of prevention (Left of Boom). On the other, the resilient bulwarks of recovery (Right of Boom).

Together, these strategies form the linchpin of a comprehensive defense. They help ensure that businesses can repel attacks. And also rise stronger from the ashes if breached.

What Do "Left of Boom" and "Right of Boom" Mean?

In the realm of cybersecurity, "Left of Boom" and "Right of Boom" are strategic terms. They delineate the proactive and reactive approaches to dealing with cyber threats.

"Left of Boom"
refers to preemptive measures and preventative strategies. These are things implemented to safeguard against potential security breaches. It encompasses actions aimed at preventing cyber incidents before they occur.

"Right of Boom"
pertains to the post-breach recovery strategies. Companies use these after a security incident has taken place. This phase involves activities like incident response planning and data backup.

Together, these terms form a comprehensive cybersecurity strategy. They cover both prevention and recovery aspects.

Left of Boom: Prevention Strategies

User Education and Awareness

One of the foundational elements of Left of Boom is employee cybersecurity education. Regular training sessions can empower staff.

Robust Access Control and Authentication

Access control tactics include:

- Least privilege access
- Multifactor authentication (MFA)
- Contextual access
- Single Sign-on (SSO) solutions

Regular Software Updates and Patch Management

Left of Boom strategies include ensuring all software is regularly updated.

Network Security and Firewalls

Firewalls act as the first line of defense against external threats. Install robust firewalls and intrusion detection/prevention systems.

Regular Security Audits and Vulnerability Assessments

Conduct regular security audits and vulnerability assessments. This helps to identify potential weaknesses in your systems.

Right of Boom: Recovery Strategies

Incident Response Plan

Having a well-defined incident response plan in place is crucial.

It should include things like:

- Communication protocols
- Containment procedures
- Steps for recovery
- IT contact numbers

Data Backup and Disaster Recovery

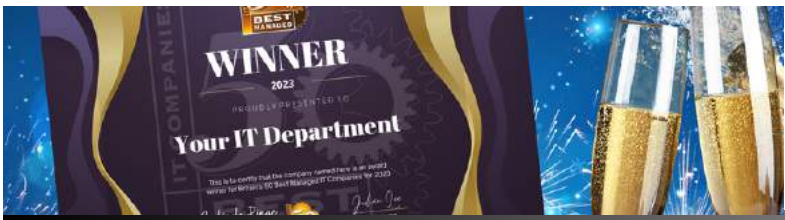
Regularly backing up data is a vital component of Right of Boom. Another critical component is having a robust disaster recovery plan.

Forensic Analysis and Learning

After a security breach, conduct a thorough forensic analysis. It's essential to understand the nature of the attack. As well as the extent of the damage, and the vulnerabilities exploited.

Legal and Regulatory Compliance

Navigating the legal and regulatory landscape after a security breach is important.



Best Managed IT Companies 2023

YOUR IT NAMED IN TOP 50 IN THE UK ONCE AGAIN.

The results of the eChannelNews Annual survey are in and Your IT have once again been named in the top 50 Managed IT companies in the UK

To enter each company completes a 200 question survey which is evaluated by a combination of human and AI.

With incredible fierce competition Your IT are very proud of achieving Top 50 status.

JANUARY / FEBRUARY 2024

BITS & BYTES

TOP DATA BREACHES OF 2023: NUMBERS HIT AN ALLTIME HIGH

The battle against cyber threats is an ongoing challenge. Unfortunately, 2023 has proven to be a watershed year for data breaches. Data compromises surged to an all-time high.

The last data breach record was set in 2021. That year, 1,862 organisations reported data compromises. Through September of 2023, that number was already over 2,100.

In Q3 of 2023, the top data breaches were:

- HCA Healthcare
- Maximus
- The Freecycle Network
- IBM Consulting
- CareSource
- Duolingo
- Tampa General Hospital
- PH Tech

Let's look at the main drivers of this increase.

1. The Size of the Surge – Data breaches in 2023 have reached unprecedented levels. The scale and frequency of these incidents emphasise the evolving sophistication of cyber threats as well as the challenges organisations face in safeguarding their digital assets.

2. Healthcare Sector Under Siege – Healthcare organisations are the custodians of highly sensitive patient information. As a result, they've become prime targets for cybercriminals.

3. Ransomware Reigns Supreme – Ransomware attacks continue to dominate the cybersecurity landscape. The sophistication of this threat has increased.

4. Supply Chain Vulnerabilities Exposed – Modern business ecosystems have an unconnected nature. This has made supply chains a focal point for cyberattacks. The compromise of a single entity within the supply chain can have cascading effects.

5. Emergence of Insider Threats – The rise of insider threats is adding a layer of complexity to cybersecurity. Organisations must distinguish between legitimate user activities and potential insider threats.

6. IoT Devices as Entry Points – The proliferation of Internet of Things (IoT) devices has expanded the attack surface. There's been an uptick in data breaches originating from compromised IoT devices.

7. Critical Infrastructure in the Crosshairs – Critical infrastructure has become a target of choice for cyber attackers.

8. The Role of Nation-State Actors – Nation-state actors are increasingly playing a role in sophisticated cyber campaigns. They use advanced techniques to compromise sensitive data and disrupt operations.

9. The Need for a Paradigm Shift in Cybersecurity –The surge in data breaches underscores the need to rethink cybersecurity strategies.

10. Collaboration and Information Sharing – Collaboration among organisations and information sharing within the cybersecurity community are critical. Threat intelligence sharing enables a collective defense against common adversaries.

MEET THE TEAM
ALICE TAYLOR
SALES COORDINATOR

Alice joined the team in December 2022 on a Graduate Apprenticeship scheme and will be taking up a new role as Sales Coordinator in 2024.

Originating from Stratford-upon-Avon, Alice moved to Nottingham to study at Notts Trent University and has made the city her home.

Alice loves a work social, even managing to persuade several staff members to take part in a 16-mile 3 peak challenge for charity last year, raising over £2,000.

As Alice has initially been focused on new business she may not be a familiair name to our existing clients but in her new role she'll be getting to know you all a lot better.

The Sales Coordinator role is focused on improving the customer service beyond the service desk.

This means we'll be able to react even more quickly to your general non-support queries, requests for new equipment etc.

TECHNOLOGY TRENDS CHANGING THE WAY WE WORK

Technology is reshaping the world of work at an unprecedented pace. From artificial intelligence to web3, from the metaverse to the hybrid work model. We are witnessing a series of technological revolutions. They are transforming how we communicate, collaborate, create, and innovate.

Let's explore some of the most impactful technology trends that are changing the way we work in 2024 and beyond.

1. Artificial Intelligence
2. Remote Collaboration Tools
3. Hybrid Work Model
4. Web3: The Decentralised Internet
5. Internet of Things (IoT) in the Workplace
6. Augmented Reality (AR) and Virtual Reality (VR)
7. Cybersecurity Advancements

These transformative technology trends are not just fleeting novelties. They are shaping the future of work.

14 HELPFUL TIPS FOR NEW YEAR DIGITAL DECLUTTERING

These days, it's easy to feel overwhelmed at the sight of an endless inbox or app library.

As the new year begins, it's the perfect time for a digital declutter. A clean and organised digital environment can help you improve your productivity. It also reduces stress. Here are some practical tips to help you declutter your digital space.

- Start with a digital inventory
- Focus on your most-used digital spaces
- Organise your files and folders
- Clean up your email inbox
- Clean up your social media
- Review your subscriptions
- Review and delete unused apps
- Clear your desktop and downloads folder
- Secure your digital identity
- Evaluate your digital habits
- Create digital detox days
- Streamline notifications
- Invest in digital tools
- Practice regular maintenance

7 HELPFUL FEATURES ROLLED OUT IN THE LATEST WINDOWS 11 UPDATES

In a world where technology constantly evolves, Microsoft stands at the forefront.

It continues to pioneer innovations. Innovations that transform how we interact with our digital universe.

The fall Windows 11 update is a testament to Microsoft's commitment to excellence. It's more than just an upgrade. It's a leap into the future of computing. Microsoft touts it as "The most personal Windows 11 experience."

Here are some of the great features recently rolled out:

- Microsoft Copilot: Your Intelligent Partner in Creativity
- Updated Apps (Paint, Snipping Tool, Clipchamp & More)
- Easy Data Migration with Windows Backup
- Microsoft Edge: A Better Browsing Experience
- Save Energy & Battery Power
- A More Personal Windows 11 Experience

HOW SMALL BUSINESSES CAN APPROACH WORKFORCE TECHNOLOGY MODERNISATION

Technology plays a pivotal role in driving efficiency, productivity, and competitiveness. For small businesses, workforce technology modernisation is both an opportunity and a challenge.

Embracing modern technology can empower small businesses. It can help them thrive in a digital era. Important benefits include improved employee retention and decreased cybersecurity risk not to mention the productivity and time-saving advantages.

Here are some steps to help your small business get started.

- Assess Your Current Technology Landscape
- Align Technology Goals with Business Objectives
- Focus on Cloud Adoption
- Invest in Collaborative Tools
- Look at Cybersecurity Measures
- Embrace Mobile-Friendly Solutions
- Look at Remote Work Options
- Consider Automation for Efficiency
- Provide Ongoing Training and Support
- Watch and Adapt to Evolving Technologies