APRIL 2023

Cirrus IT Services

TECH TALK

"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!

- **Scott Magee**
Managing director

DATA BACKUP IS NOT ENOUGH

The need to back up data has been around since floppy disks. Data loss happens due to viruses, hard drive crashes, and other mishaps. Most people using any type of technology have experienced data loss at least once.

There are about 140,000 hard drive crashes in the US weekly. Every five years, 20% of SMBs suffer data loss due to a major disaster. This has helped to drive a robust cloud backup market that continues to grow.

But one thing that's changed with data backup in the last few years is security. Simply backing up data so you don't lose it, isn't enough anymore. Backing up has morphed into data protection.

What does this mean?

It means that backups need more cybersecurity protection. They face threats such as sleeper ransomware and supply chain attacks. Cloud-based backup has the benefit of being convenient, accessible, and effective. But there is also a need for certain security considerations with an online service.

Companies need to consider data protection when planning a backup and recovery strategy. The tools used need to protect against the growing number of threats.

Some of the modern threats to data backups include:

- **Data Center Outage:** The "cloud" basically means data on a server. That server is internet accessible. Those servers can crash. Data centers holding the servers can also have outages.
- **Sleeper Ransomware:** This type of ransomware stays silent after infecting a device. The goal is to have it infect all backups. Then, when it's activated, the victim doesn't have a clean backup to restore.
- **Supply Chain Attacks:** Supply chain attacks have been growing. They include attacks on cloud vendors that companies use. Those vendors suffer a cyberattack that then spreads throughout their clients.
- **Misconfiguration:** Misconfiguration of security settings can be a problem. It can allow attackers to gain access to cloud storage. Those attackers can then download and delete files as they like.

What to Look for in a Data Protection Backup System

Just backing up data isn't enough. You need to make sure the application you use provides adequate data protection. Here are some of the things to look for when reviewing a backup solution.

Ransomware Prevention

Ransomware can spread throughout a network to infect any data that exists. This includes data on computers, servers, and mobile devices. It also includes data in cloud platforms syncing with those devices.

95% of ransomware attacks also try to infect data backup systems.

It's important that any data backup solution you use have protection from ransomware. This type of feature restricts automated file changes that can happen to documents.

Continuous Data Protection

Continuous data protection is a feature that will back up files as users make changes. This differs from systems that back up on a schedule, such as once per day.

Continuous data protection ensures that the system captures the latest file changes. This mitigates data loss that can occur if a system crashes before the next backup. With the speed of data generation these days, losing a day's worth of data can be very costly.

Threat Identification

Data protection incorporates proactive measures to protect files. Threat identification is a type of malware and virus prevention tool. It looks for malware in new and existing backups. This helps stop sleeper ransomware and similar malware from infecting all backups.

Zero-Trust Tactics

Cybersecurity professionals around the world promote zero-trust security measures. This includes measures such as multi-factor authentication and application safelisting.

HP ProDesk G400 Mini PCs - SALE!

Get your hands on some HP ProDesk Mini PCs at an unbeatable price, directly through our shop.

These machines are perfect as a lightweight workhorse, boasting a powerful 9th generation Intel Core i3 processor and 8GB RAM.

Don't miss out, these units are available now for just £225! (ex VAT - While stocks last.)

Get them here: https://www.cirrusits.co.uk/product/hp-prodesk-g400/

WHY YOU NEED A PASSWORD MANAGEMENT TOOL - BITWARDEN VAULT

We all know how hard it is to keep track of passwords these days. We're all used to being told by our IT & Cyber Security teams that we should be using separate, complex passwords for each site, system and service that we use. But how do you possibly keep track of so many passwords in an ever growing digital landscape?

It's time for your business to put its trust into our top of the range Password Management solution: Bitwarden.

Bitwarden is a fully comprehensive suite of tools to help you store & manage your passwords, as well as password and account security. Share passwords across the company, or have each member of the team store them in their own private vaults - or use a mixture of both!

Here at Cirrus, we recognise that security and trust are paramount; so keep reading to find out how Bitwarden assures both.

Why should I trust Bitwarden with sensitive information?

All of the source code running Bitwarden is vetted and improved by experts and the community - providing Open Source Security assurance.

In addition, Bitwarden & its services are fully HIPPA and GDPR compliant, as well as offering the reassurance that all data sent to and from the services is encrypted at both ends.

We trust Bitwarden as our Password Management tool of choice, and so should you.

What else is included, other than the Password Vault?

As well as offering an ultra-secure vault to store company & individual passwords, Bitwarden also includes several tools to help you maintain password & account security with minimum effort:

1. Bitwarden Send - Send is a secure system to send passwords via many methods of communication through link sharing. Simply enter the information you would like to share, set security constraints, and copy & send the link to the information.
2. Password Generator - Coming up with a secure password has never been easier thanks to Bitwarden's generator, which can generate passwords of infinite lengths and complexities (and in different formats such as pass phrases!)
3. Data Breach Checking - Quickly scan all of your accounts and passwords to find out whether they have been involved in any known data breaches, allowing you to respond quickly to potential threats before they occur.
4. Weak & Reused Passwords - Automatically check whether any of the passwords in your vault are of a weak standard or have been reused.

What's the benefit of using a password manager?

Password hygiene is a key part of Cyber Security, so making it easier on your staff to follow best practice in this area is always a win-win scenario; let's be honest, how many of us really use separate passwords for every account, and how much time do your IT team spend resetting forgotten passwords?

How much does it cost and can I get a quote for my team?

Bitwarden is one of those tools that hits soft on the pocket, but hard on the benefits. We offer two levels of license for this product (Teams and Enterprise), both coming in at $5 or less per month!

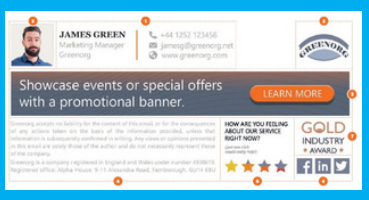
You can find out more by visiting: **CirrusITS.co.uk/Password-Management**

Or, you can email us at hello@cirrusits.co.uk to arrange a chat with one of our friendly team.

EMAIL SIGNATURES... WHAT A PAIN... NOT ANY MORE! - EXCLAIMER CLOUD SIGNATURES

Email Signatures are one of the most time consuming parts of business brand management. For most companies, or rather those who don't employ a centralised management solution, hours and hours can be spent on ensuring that all staff are using the same style & quality of Email signature, containing just the right amount and type of information.

With our fantastic Email signature management solution, Exclaimer Cloud, all of this stress & pain can be taken away.



Exclaimer invites you to use its intuitive visual interface, built into a powerful Web App, to design & manage all of your staff's signatures from one location, freeing up your time to focus on the important things.

On top of this centralised management structure, the system boasts the ability to pull in data & integrate with Office 365 using 'Dynamic Fields'.

What are Dynamic Fields?

Dynamic fields are what allow you to design one signature, and apply it to everyone, with ease. When creating a signature, instead of typing someone's name, simply select the 'Name' field, which will then automatically be filled with user information from Office 365 as emails are sent.

You can do this with a wide variety of information, such as address and telephone number, saving you valuable time and effort.

Find out more...

To find out more about this invaluable service, head over to our website:

cirrusits.co.uk/exclaimer-cloud-signatures

EVERY COMPANY IS NOW A TECHNOLOGY COMPANY

Whether you sell shoes or run an accounting firm, you need some type of technology to operate. Today's companies aren't just in the business of selling their own goods and services anymore. They also must master various types of digital tools.

1. Technology Is a Critical Part of Business
2. Customers Expect an Excellent Digital Experience
3. Employees Need Devices to Drive Productivity
4. AI & Automation Help Companies Stay Competitive
5. Information Is Being Generated at a Rapid Pace
6. Vendors/Suppliers Are Leaving Legacy Systems Behind
7. It's Difficult to Grow Without Tech Innovation
8. Business Continuity Needs

6 STEPS TO EFFECTIVE VULNERABILITY MANAGEMENT FOR YOUR TECHNOLOGY

Technology vulnerabilities are an unfortunate side effect of innovation. When software companies push new updates, there are often weaknesses in the code. Hackers exploit these.

Software makers then address the vulnerabilities with a security patch. The cycle continues with each new software or hardware update.

61% of security vulnerabilities in corporate networks are over 5 years old.

- Step 1. Identify Your Assets
- Step 2: Perform a Vulnerability Assessment
- Step 3: Prioritize Vulnerabilities by Threat Level
- Step 4: Remediate Vulnerabilities
- Step 5: Document Activities
- Step 6. Schedule Your Next Vulnerability Assessment Scan

WINDOWS 8.1 JUST LOST ALL SUPPORT. HERE'S WHAT YOU NEED TO KNOW

The latest operating system to lose all support is Windows 8.1. Microsoft released the OS in 2013, and it was officially retired on January 10, 2023. Microsoft issued the following warning for companies:

"Continuing to use Windows 8.1 after January 10, 2023 may increase an organization's exposure to security risks or impact its ability to meet compliance obligations."

Here are a few facts you should know:

- The OS Will Still Technically Work
- Your System Will No Longer Receive Security Patches
- Options for Upgrading are Windows 10 or 11

What Happens if you don't upgrade?

- Security & Compliance Issues
- Slowed Productivity
- Incompatibility With Newer Tools

TECHNOLOGY TRIVIA TIME

Each month you have a chance to win an Amazon Gift Card! Our March competition winner (randomly selected from correct entries) was:

Chris Greenwood,
Capll Ltd.

Congratulations, Chris!

The question this month is:

In what video game series did Microsoft's virtual assistant Cortana make her debut?

Email us at hello@cirrusits.co.uk with the correct answer by 15th April 2023 for your chance to win! Good Luck!