THREATS TO DATA SECURITY HAVE EVOLVED

Over the past year there has been an exponential rise in the use of cloud storage. Driven by the pandemic, businesses of all sizes have made rapid changes to their IT infrastructure to enable remote or hybrid working for their employees – is the shift to a cloud-first strategy jeopardising security in the process, resulting in an increased risk to cyber attacks?

The current cyber threats to data security are impacting businesses of all sizes and all industries, and the threat is very real, therefore data security must be at the cornerstone of the business agenda.

But with the fast-evolving landscape of incoming threats, how can a business possibly maintain the security of its most precious commodity – its data?

The big issue is that the threats are getting relentlessly more sophisticated, at a significantly fast pace, putting businesses on an immediate back foot. But could there be a simple solution? Does a solution already exist to help mitigate risks that is so simple that it gets dismissed with a quick swipe?

In this whitepaper we will discuss:

- How has data security evolved?
- Where cyber attacks start
- How much understanding do employees have about cyber threats?
- Putting data security at the top of the agenda
- Who is the guardian of your data?
- A simple solution to ransomware attacks
HOW HAS DATA SECURITY EVOLVED?

The approach and focus on the digital environment has shifted from digitalising systems and focusing on the technology, through to concentrating on the controls placed around data and how to ensure its protection.

This has come about through the relentless increase in cyber attacks that are designed to access business data, whether payroll information, customer payment information, intellectual property, contracts and client lists or employee personal records.

Any business data is of value to the hacker, the higher the sensitivity, the higher the value. And don’t be fooled, hackers collaborate to share collected data obtained by a number of tried, tested and successful methods. To think that because the business has survived one malware attack and actions were taken to tighten data security that another wouldn’t be possible is futile. Hackers are creative and therefore the threats are evolving at pace, putting the majority of businesses on a back foot.
WHERE CYBER ATTACKS START

It starts with us as individuals - human error accounts for over 90% of data breaches. Coupled with the fact that 94% of cyber attacks start with a phishing email, safeguarding data appears to be out of control. In the UK alone, more than 11,000 UK government-themed phishing campaigns were taken down in 2020 – twice the number as 2019.

Breaches can result in loss of sensitive data, massive fines, loss of customers and profits, adverse publicity and job losses. The sad but true reality of simply clicking on a link in an email.

By sending a phishing email, a hacker is looking to trick individuals into sharing data that could enable them to login to the business network and install malware, or a bogus business looking to scam the business out of money. They may send an email from a service provider known to you asking you to click on a link. From here they may have obtained the access needed to install malware or a virus on your system. However, they could be asking employees to click on a link and enter login credentials, then they have obtained their goal - to get access to confidential data.
HOW MUCH UNDERSTANDING DO EMPLOYEES HAVE ABOUT CYBER THREATS?

In the 2021 iStorage backup survey, we found that over 88% thought their employers could do more to implement tighter cyber security practices. This is coming from employees – not the CEO or CTO – individuals know they have an important part to play, but this must be enforced through governance and compliance policy implementation and, more importantly, ensuring that everyone understands what this means to them.

77% DO NOT UNDERSTAND THE TERM ‘RANSOMWARE’
70% DO NOT UNDERSTAND THE TERM ‘MALWARE’
65% ADMIT TO HAVING LOST DATA
99% STATE THAT DATA LOSS OR THEFT IS OF CONCERN

These insights reveal that there is a huge opportunity to get the workforce advocating for the security of business data and reduce threats through cybersecurity awareness training. They appear to understand the concern over data security, but have little, or no knowledge of cyber threats and therefore are unintentionally putting the data, and therefore the business at risk.
PUTTING DATA SECURITY AT THE TOP OF THE AGENDA

Cyberterrorism is now considered a national-risk by many governments. Nations tend to rally together against conventional terrorism, but for some unknown reason cyberterrorism is left for others to deal with. But who? The government, CTO’s and CEO’s? Everyone has a responsibility towards keeping data secure – whether personal or business related.

However, in June 2021, President Joe Biden started to lead the charge on cyberterrorism and issued an executive order to ‘improve the nation’s cybersecurity’. The executive order focused on data security:

- **60 DAYS:** Get things as secure as possible and remediate cyber risk
- **180 DAYS:** All need to adopt multi-factor authentication (MFA) and encryption both at-rest and in-transit
- **180 DAYS:** Implement and test an incident response plan. Test your contingency plans to ensure that critical functions can continue to operate during a cyber attack

This is the type of awareness and action that is needed across the world, across businesses of all sizes, in all industries in order to combat the threat. Taking immediate steps to enforce organisational cyber security policies, maintain updates to technical applications and devices, implement a robust backup process and ongoing training programs for employees will help raise the shield against cyber threats.
WHO IS THE GUARDIAN OF YOUR DATA?

Organisations place their data in the cloud with the belief that it will be safeguarded. However, the fact that the data has been placed on another hard drive in a data centre, outside of the organisation's control, is often overlooked. Data Centre's are as vulnerable to the threat of cyber attacks, fire and theft as much as any organisation, therefore businesses must manage control over their data – leaving the security in someone else's hands and not having a recovery plan in place is going to be detrimental and irreversible in the event of a ransomware attack.
A SIMPLE SOLUTION TO RANSOMWARE ATTACKS

Simple, affordable and secure – encrypted hardware devices. Here’s how it works in relation to a ransomware attack:

Ransomware groups use a variety of techniques to get into a business’s network, with the aim of stealing and encrypting your data. When the business data is encrypted, they will demand a payment in return for the decryption key. Upon receipt of the payment, the cybercriminals may then threaten to expose confidential or sensitive data unless the business makes a second payment – this is known as ‘double extortion’.

If an organisation runs regular backups, ideally to a secure offline data storage device, in the event of a ransomware attack, they can simply restore data from their most recent backup, thus reducing downtime, disruption, stress, adverse publicity and the need to pay a hefty fine.

Implement an authorised removable media policy to control the use of USB devices. iStorage USB encrypted devices are configured with a unique VID/PID allowing whitelisting to meet internal corporate requirements.

When sensitive data is stored offline on an iStorage device, it is immediately scanned using iStorage DriveSecurity software which detects and eliminates Viruses, Spyware, Trojans, Worms, Rootkits, Adware and other security threats before they are copied to an iStorage drive for ultimate data protection.
iStorage was founded in 2009 and is the world leader in encrypted hardware data storage solutions. Our range of PIN authenticated hardware encrypted data storage devices provide organisations with a simple solution for secure backups. As the data is kept away from the system, it is not vulnerable to ransomware attacks.

We provide businesses with the opportunity to evaluate our award winning devices for free before incorporating it into their overall data security infrastructure.

Find out more at:
www.istorage-uk.com
www.istorage-usa.com
www.istorage-fr.com
www.istorage-de.com

Contact us:
info@istorage-uk.com
+44 (0) 20 8991 6260