Kingston TECHNOLOGY

USB storage: Does hardware encryption prevent risks?

#KingstonIsWithYou

USB storage: Does hardware encryption prevent risks?

Foreword and contents

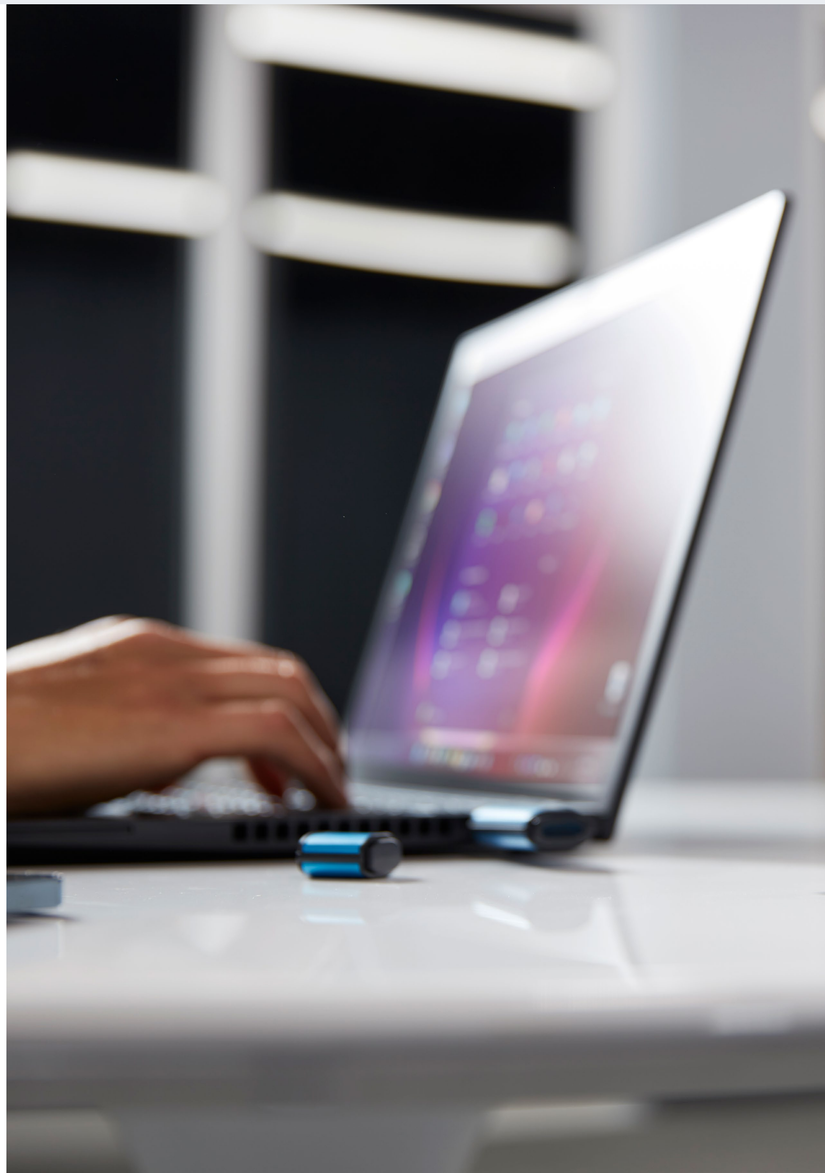
Cybersecurity is more of a concern for businesses than ever, but too many organisations are uninformed about and underprepared for cybersecurity threats. In the United States, only 50% of businesses have a cybersecurity plan in place; of those, 32% haven't updated their cybersecurity plans since the start of the COVID-19 pandemic, which saw many organisations moving to remote or hybrid working models according to UpCity. And the frequency of cyberattacks is only increasing - globally, the number of businesses hit with ransomware attacks increased from 37% in 2020, to 66% in 2021[1].

Compromised cybersecurity can have devastating effects on a business - aside from the monetary cost of cyberattacks, the loss of data, safety, and reputation can negatively impact organisations in many ways, both in the short and long term.

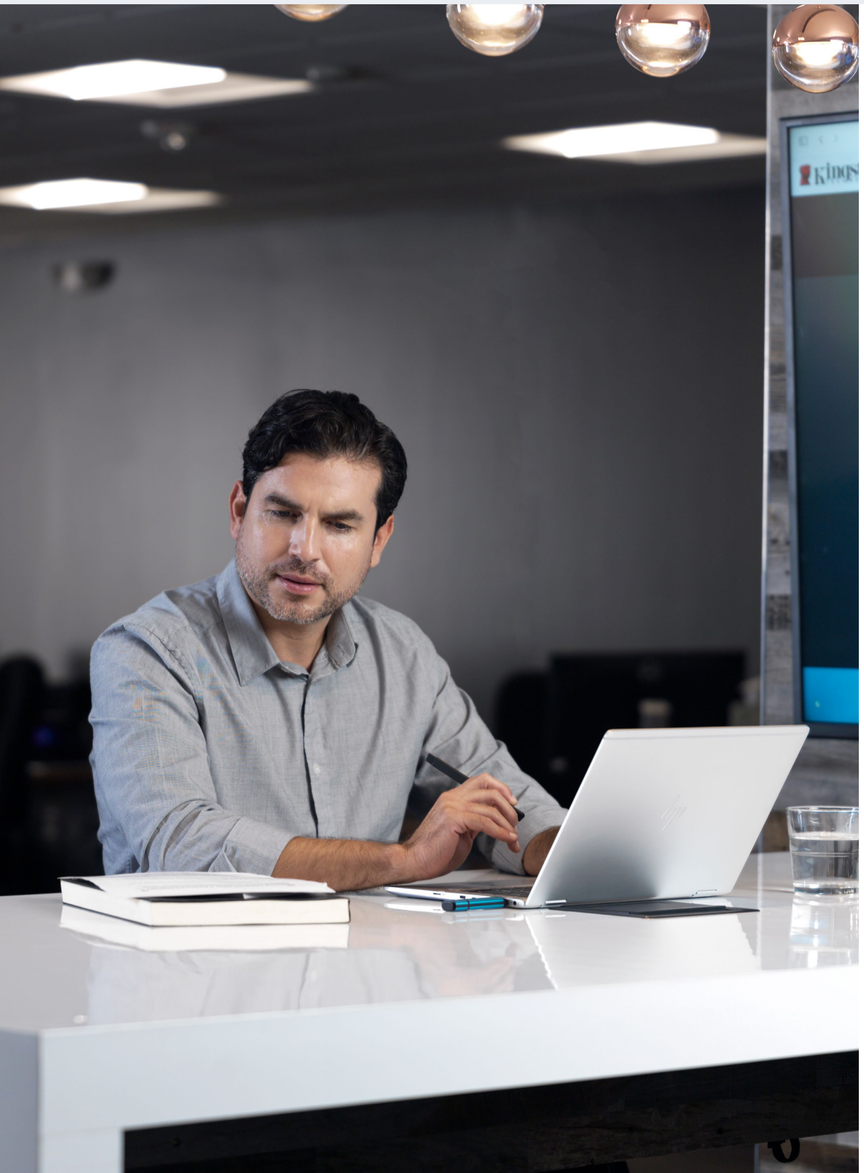
One common vehicle for cybersecurity threats are USB drives. These have become ubiquitous in many organisations because of their simplicity - just plug them into a machine and they're ready for use. However, it is exactly this simplicity that leaves USB drives so vulnerable to attacks: all it takes is one misplaced or stolen drive for a malicious actor to access potentially sensitive data. This is where encryption can play a significant role in making USB drives safe for use and mitigating any associated risks for the individual and the organisation. In this eBook we offer answers to the following key questions:

- Why are encrypted USBs so crucial in protecting against cyberattacks?
- Where are organisations making themselves vulnerable?
- What can they do to protect themselves?

Table of content	Pages

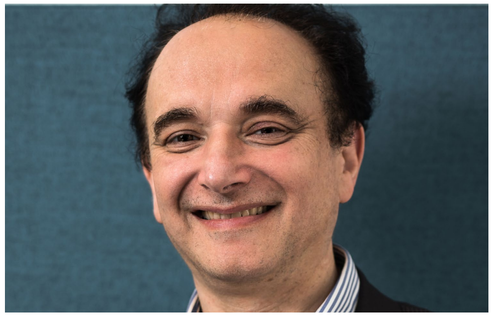


USB storage: Does hardware encryption prevent risks?



Contributors

This eBook has been created with leading industry figure in IT and emerging technologies, along with our own technical expert.



David Clarke

David is recognised as one of the top 10 influencers by Thompson Reuter's "Top 30 most influential thought-leaders and thinkers on social media, in risk management, compliance and reg-tech in the UK" and is in the top 50 list of Global Experts by Kingston Technology.

Pasi Siukonen

Pasi is responsible for leading a team of experts supporting Kingston departments such as PR, Marketing, Field Sales, Technical Support and Customer Service on Kingston products. His primary product focus is Flash and SSD product lines.

The difference between commodity and encrypted drives

While commodity (unencrypted) drives are extremely simple to access and use, hardware encryption adds several layers of security - both physical and digital - that make USB storage far more secure. The easy availability, low cost and portability of commodity unencrypted drives means that while they are very convenient for the user, they are also convenient for malicious actors aiming to steal sensitive data, introduce malware or ransomware into a company network, and more. As USBs are used so often, the opportunities for cyberattacks are many. There are two main risks associated with commodity drives:

- **Ransomware attacks:** these USB-based attacks involve introducing malware into company networks, holding company information and/or systems ransom by encrypting them. These are often caused by BadUSBs and have become the most prominent type of malware.
- **Stolen data:** all it takes is a lost, stolen, or unattended drive without the appropriate security measures in place for a malicious actor to easily access the data stored on the drive - whether it's customer information, source code, or sensitive financial and performance data.

BadUSB – is an attack that can exploit the vulnerability of USB drives with unprotected firmware, which then can be programmed with malicious software. These malicious tools are incredibly common and easily available to cyber criminals, yet awareness about these tools remains low, making these attacks all too easy to carry out by replacing a commodity drive's firmware with a hacked firmware where the USB drive can masquerade as a keyboard and basically run scripts to attack the firewall. As so many cyberattacks are carried out through unsuspecting insiders with or without malicious intent, it is incredibly important that businesses use encrypted drives that utilise protected, digitally-signed firmware to prevent these attacks, which can reduce the chances of success for cyber criminals.

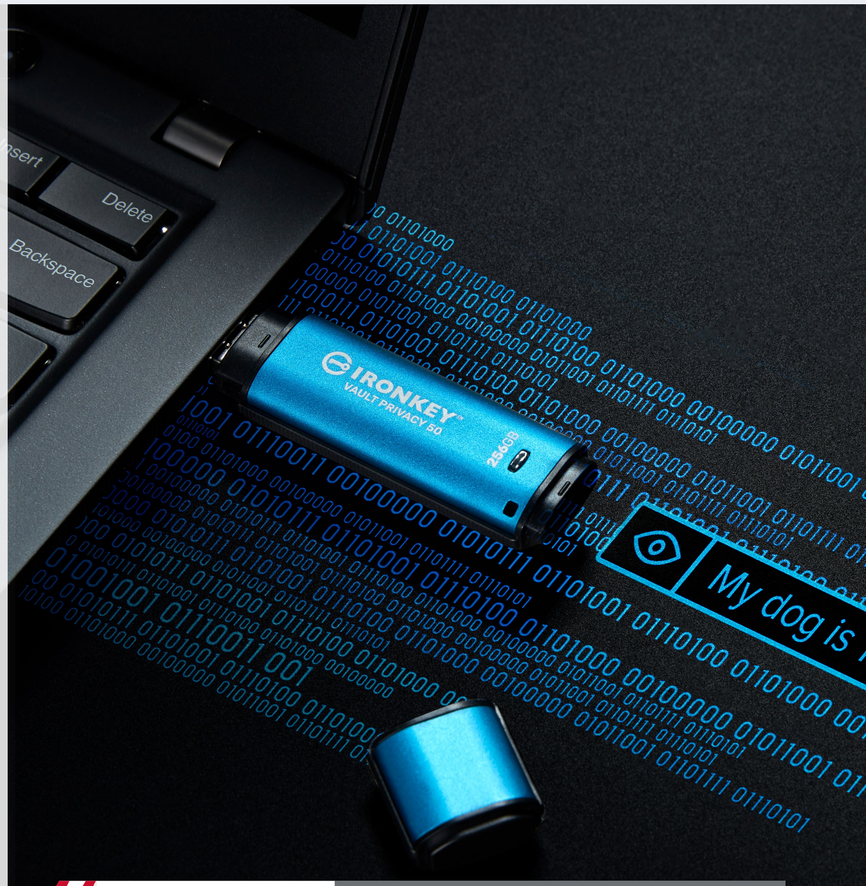
> **The cost of rebuilding infrastructure, and maybe paying the ransom and other extortion, is massive compared to the costs of managed USBs. - David Clarke**

Why use encrypted USBs?

Encrypted drives are specifically designed to protect the data contained inside, as well as any devices the drive might be connected to, making them valuable tools in any organisation's IT arsenal. As cybersecurity threats have become more advanced, so have the features of encrypted drives, enabling them to stay ahead of cyber criminals looking to exploit these devices. As seen with the Kingston IronKey™ hardware-encrypted product line, features such as AES 256 bit encryption in the strongest XTS mode, rugged and tamper-resistant casing, digitally-signed firmware, virtual keyboards, complex or passphrase modes and more have been developed and added over the years to ensure that users are well and truly protected from all manner of attacks.

Because cyber risks are so often poorly understood, many businesses will choose to use commodity drives, despite the various vulnerabilities these bring along. Their ease of availability, low cost and the use of software encryption play a role here, as does the lack of a corporate approval process for flash drives. Too often there are no organisational best practice policies or processes to comply with various IT and cybersecurity standards, such as ISO27001, GDPR, SOC2 and WISP governmental best practices. This means that risks are often assessed based on opinion, rather than evidence - leaving many organisations vulnerable to attacks.

While some may use commodity drives with existing software encryption tools, this can often be a false economy as many software encrypted drives can be hacked with free or paid tools available on the Internet to anyone. Software encryption can also be removed from a drive with a simple reformatting of the drive by a user for convenience or to use the drives on non-supported OS platforms. While hardware-encrypted USBs have always-on encryption that cannot be turned off, they are fit for purpose; and are built to be tamper-resistant, tamper-evident, and use digitally-signed firmware to ensure the authenticity and integrity of the drive. Limiting password attempts (Brute Force attack protection) and virtual keyboards (protects against keylogging and screenlogging) are two more features of encrypted drives such as IronKey VP50, which mean it complies with industry best practices against malicious actors who aim to extract passwords from unsuspecting users.



> If the IronKey drive detects that the firmware has been tampered with, it will brick the drive and not boot up, thereby enhancing cybersecurity.
> - Pasi Siukonen

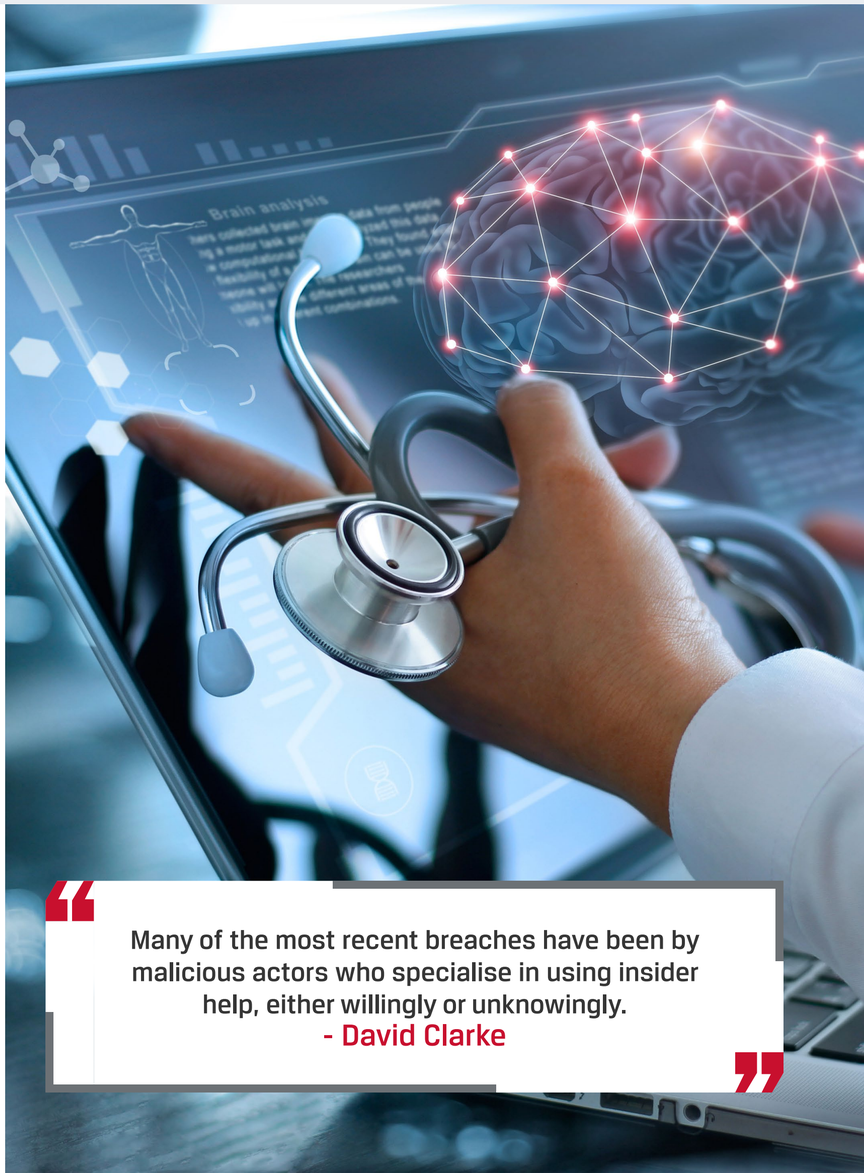
Who is at risk?

Really, any companies that are unable to control their USB access are at risk - and often, they are not aware of exactly what those risks are. However, there are factors that can make certain companies more attractive - and vulnerable - targets for cyberattacks.

For companies in the healthcare and financial sectors, their data is not only much more attractive to cyber criminals, but it also impacts both the organisations and their customers in more severe ways. In the UK, a 2017 cyberattack that targeted the NHS caused over 19,000 appointments to be cancelled, and cost the NHS £92 million in lost output, as well as costs to restore data and systems. Not only did this prevent the affected patients from receiving healthcare, but the NHS was heavily criticised for not responding quickly or substantially enough to previous cyber threat warnings. While all organisations should be up-to-date and well-informed about cybersecurity, those that deal with sensitive information - particularly special category data - should be doubly vigilant concerning cyber risks.

The higher the value of the company, as measured by turnover, the greater the reward for malevolent actors - and therefore, the greater the risk they face from cyber threats. However, that doesn't mean that smaller organisations shouldn't be concerned about cybersecurity; while enterprises may be more attractive targets for attacks, they often also have the resources and dedicated staff to address cyber threats. On the other hand, many SMBs do not have dedicated cybersecurity teams and make exceptions for senior executives to avoid USB management, making them particularly vulnerable with devastating outcomes. Some studies show that small and medium businesses are actually targeted more for cyberattacks.

The risk is even greater for employees in senior executive positions; these individuals are easily traceable and often have executive privilege at their organisations, meaning that cyber controls - such as USB management procedures - are not applied to them, making them lucrative targets for cyber criminals. This is where always-on hardware-encrypted drives, along with being well-informed on cybersecurity and following best practices and processes, can go a long way in reducing risk and protecting against attacks.



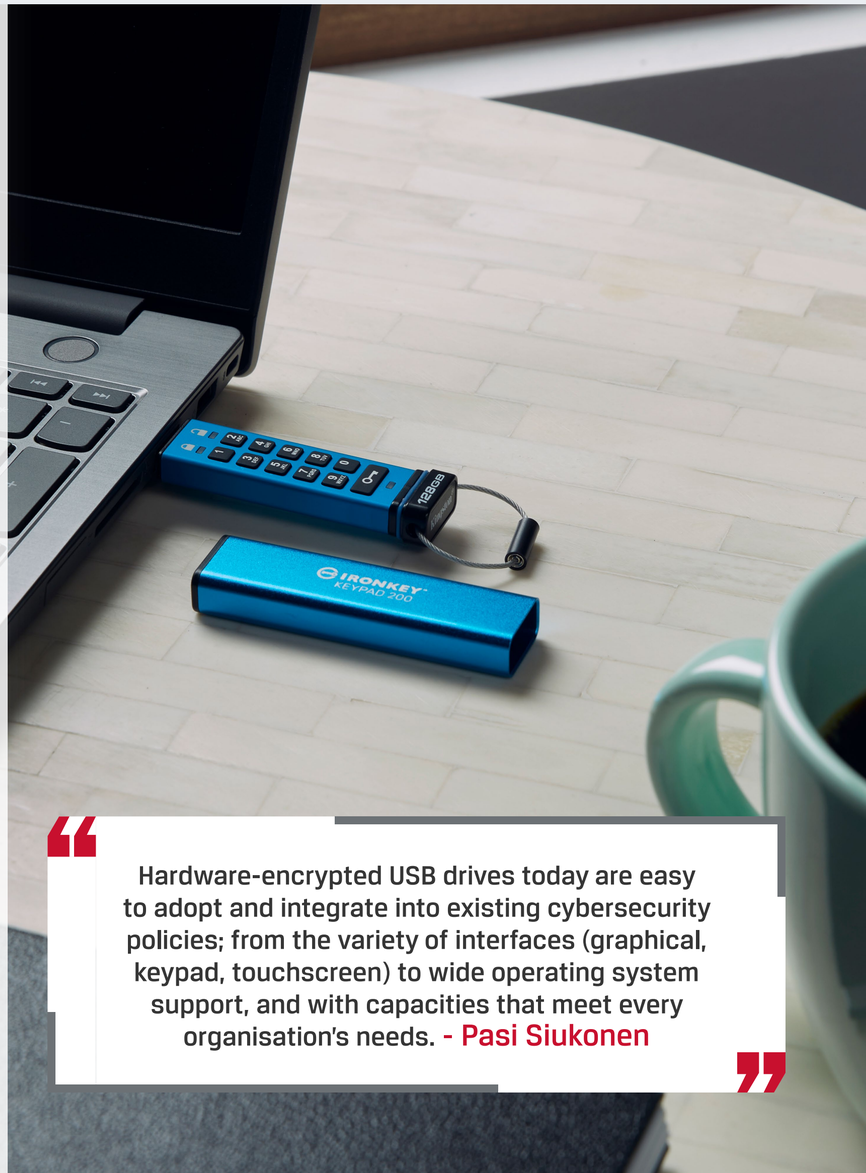
> Many of the most recent breaches have been by malicious actors who specialise in using insider help, either willingly or unknowingly.
> - David Clarke

Who is at risk?

> Organisations are not doing enough to counter cybersecurity threats. - David Clarke

The supply chain is another potential point of vulnerability for organisations, and supply chain attacks are all too common. In 2013, US retailer Target was hit with one of the largest data breaches in retail history, exposing the debit and credit card information of over 40 million customers. Although Target itself was very concerned about cybersecurity, having just installed an extensive cybersecurity system 6 months prior to the attack, the attackers had infiltrated one of Target's third-party suppliers, and gained access to Target's main data network through them. All in all, 90 lawsuits were filed against Target, and the company lost $61 million in responding to the breach; while they may not have been directly responsible for the attack, this weakness in their supply chain's cybersecurity was enough to cause damage, both financial and reputational.

Employee workarounds can also be a source of vulnerability. While these workarounds can enable employees to be more effective in their day-to-day work, far too often basic security processes and best practices will be overlooked, such as password management. Although guidance from the NCSC and CISA is fairly straightforward, it is often harder to implement in practice, especially from team members who are not familiar with IT and cybersecurity. While having a dedicated cybersecurity team can certainly help, giving employees the right tools - such as hardware-encrypted drives - can go a long way in mitigating risks from employee workarounds.



> Hardware-encrypted USB drives today are easy to adopt and integrate into existing cybersecurity policies; from the variety of interfaces (graphical, keypad, touchscreen) to wide operating system support, and with capacities that meet every organisation's needs. - Pasi Siukonen

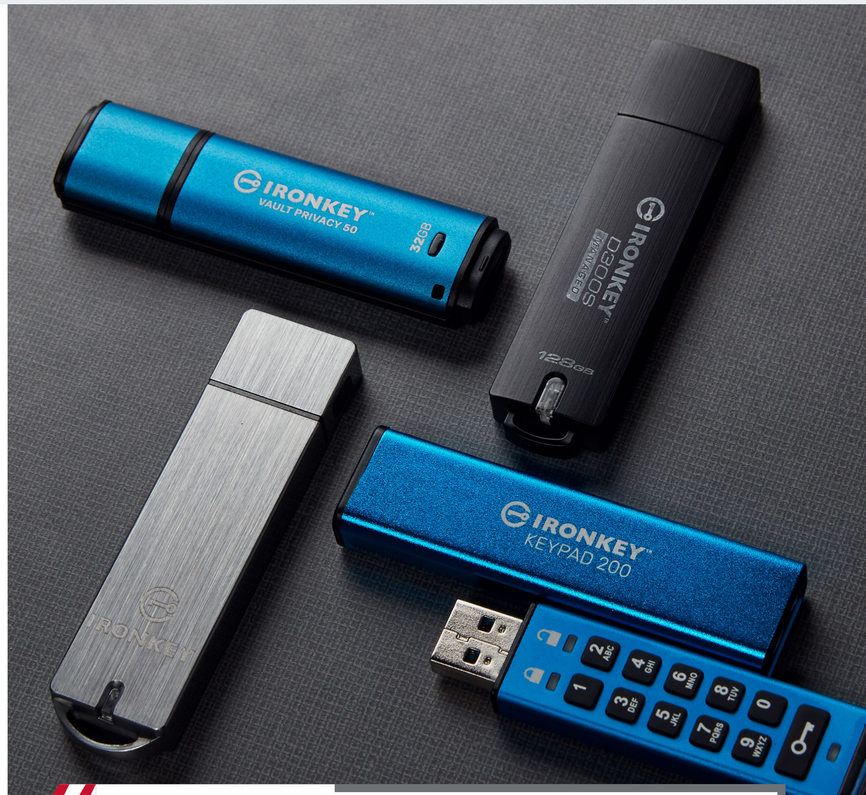
How can organisations reduce the risk of cyberattacks?

From an organisational standpoint, there are a number of things that can be done to secure endpoints and protect data. Without GRC (Governance, Risk, Compliance) cybersecurity is bound to fail - so being familiar with and following processes is incredibly important for businesses to protect themselves. Having robust endpoint security software in place can also neutralise a number of cyber threats, along with being as responsive as possible when it comes to patching any security vulnerabilities.

> **Whether to adopt enforced encryption policies or not is as significant or possibly even more significant question for risk management as it is for whether you choose to back up your data ... or not.**
> - Pasi Siukonen

On an individual level however, encrypted hardware can drastically reduce vulnerabilities against cybersecurity threats. With the rise - and endurance - of remote and hybrid work, especially coupled with the increase in cyberattacks in the last year, ensuring that employees at every level of the organisation are securely handling, transferring, and reading company data is becoming more important than ever. Hardware-encrypted USBs allow users to keep benefitting from the portability and simplicity of flash drives, while also greatly reducing the risk associated with them; while a misplaced or stolen commodity drive can mean lost data, money, reputation, and more, hardware-encrypted drives are designed to protect sensitive data from a wide range of attacks. And as cyber criminals develop new ways of attacking, encrypted drives will continue evolving to meet these new challenges.

All in all, the cost of dealing with a cyberattack can be huge. And indeed, while the adoption and use of encrypted drives on an organisational level may require a more involved approval and setting up, it can save the company a lot of money - both in terms of extortion costs, and lost revenue due to a damaged reputation - in the long run. Just the legal costs alone of a breach can easily pay for the added cost of hardware-encrypted USB drives.



> **Through long-term commitment to providing great encrypted USB solutions, Kingston's portfolio allows any organisation to meet their cybersecurity configurations - industry standard enforced hardware-encryption, endpoint policy compliant designs, device management capabilities.**
> - Pasi Siukonen

Summary

At Kingston, we are always looking at the developments in the cybersecurity space, ensuring that our IronKey encrypted drives are up to date with the latest requirements and meeting the cybersecurity needs of organisations, both large and small. As cybersecurity continues to be a growing concern globally, we're confident that with the right tools and knowledge at their disposal, organisations can be well-equipped to meet these challenges head on, while protecting themselves, their employees, and their customers.

1. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021

About Kingston

With over 35 years' experience, Kingston has the knowledge to identify and resolve your mobile data challenges – making it easy for your workforce to work securely without compromising your organisation.

#KingstonIsWithYou