The State of USB Data Protection 2019

Employee Spotlight

Data protection is critical across industries – but the obstacles to ensuring it are more challenging than ever. How can organizations and their employees protect confidential information? A recent survey of nearly 300 IT employees from industries including education, finance, government, healthcare, legal, retail, manufacturing, and power and energy reveals that:

(9 out of 10)

employees surveyed currently use USB devices at work

(9 out of 10)

employees say that USB device encryption should be required at work

(6 out of 10)

employees use non-encrypted USB devices at work

This report – the first in a two-part series – provides insight on the benefits, policies and business drivers of USB drives with a focus on employee USB drive usage. The results are clear: encryption is necessary for data protection above regulatory compliance, and when USB drives are deployed, they too must be encrypted.

The State of USB Data Protection 2019

Employees Are Driving USB Adoption – But Aren't Following Best Security Practices

With the ever-increasing frequency and severity of data breaches, companies need to vigilantly monitor the data flowing into, out of, and across the organization. We know from the survey results that most employees use USB drives, but are companies enforcing their own policies and are employees adhering to best security practices?

87% of respondents confirmed their organization uses USB drives *and...*

68% of respondents confirmed that employee choice was the primary reason.

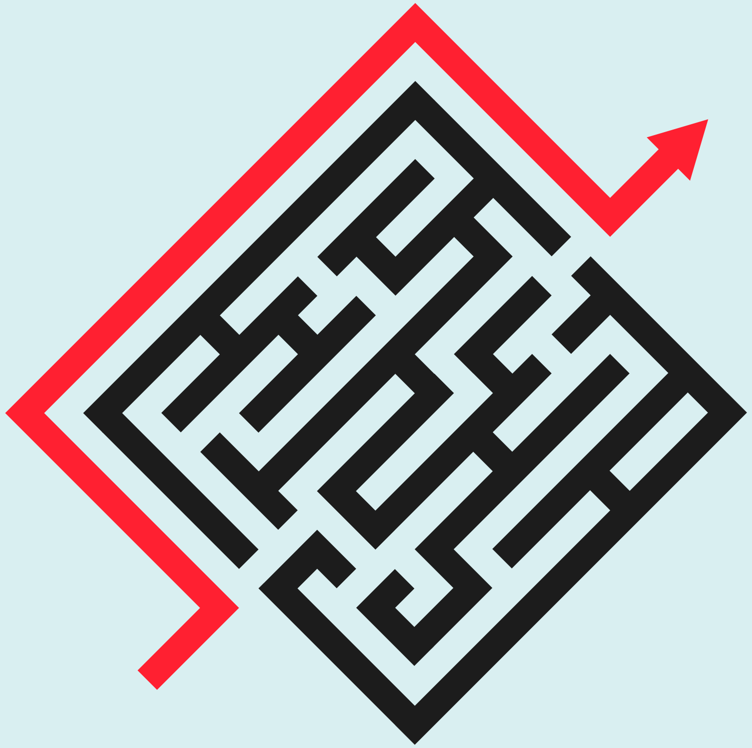
91% of respondents confirmed say USB drive encryption should be mandatory at work, *yet...*

58% of respondents confirmed they use non-encrypted USB drives at work regularly!

Takeaway:

Although USB drives are used by almost every employee – and USB usage is primarily driven by employee preference – employees begin ignoring security best practices as soon as they get their hands on a USB drive. For evidence, look no further than the device itself: nearly every employee is aware of the importance of using encrypted USB drives, but more than half of them regularly use non-encrypted USB drives. This leaves their organization – including confidential company, employee and client information – exposed and unprotected.

The State of USB Data Protection 2019



Employees Are Increasingly Taking Security Shortcuts

Considering the overwhelming majority of employees use USB drives, how closely are employees following existing policies for secure use of USB drives? By comparing these 2018 survey results against Apricorn's 2017 State of USB Data Protection survey results, several troubling trends emerge…

- **Most organizations (64%) have a policy outlining acceptable use of USB devices, but 64% of respondents said their employees use USB drives without obtaining advance permission to do so (compared to 57% in 2017)**
- **In 2018, 58% of employees used non-encrypted USB drives such as those received "free" at conferences – compared to 56% in 2017**
- **Nearly half (48%) of employees lost USB drives without notifying appropriate authorities about the incident – compared to 39% in 2017**
- **Lost USB drives were a particular problem in the retail industry – 14% of respondents confirmed that more than 75% of employees had lost a USB drive over the past year**

Takeaway:

Unfortunately, employees have demonstrated that they will consistently act against security best practices when it comes to USB drive usage. This is primarily driven by employees taking security policy shortcuts, such as failing to gain permission to use USB drives, as well as failing to notify management about lost or stolen devices. And not only are employees taking these shortcuts, but they are doing so at a higher rate than in previous years – underscoring that employee non-compliance is trending in the wrong direction. Considering there are now more threats than ever – and these threats are more sophisticated and costlier than ever – it is imperative that organizations educate their employees on the risks of not adhering to USB drive best practices and enforce policy compliance.

The State of USB Data Protection 2019

Conclusion: In today's era of ultra-sophisticated security threats that are growing in both scope and volume, it's critical that organizations – especially those that frequently work with intellectual property and other highly confidential information – provide their employees with secure USB drives that prevent organizations' worst nightmares: data breaches and loss of sensitive data. With 9 out of 10 employees using USB devices today and nearly 60 percent of them regularly using non-encrypted USB devices – not to mention the alarming statistics around employees' failure to follow best practices – it's time for companies to assert control over their employees' use of USB drives. Organizations would be wise to provide employees with USB drives that include the following:

- *Software-free authentication and encryption (for efficiency and cross-platform compatibility)*
- *Military-grade on-the-fly 256-bit hardware encryption*
- *Embedded keypad (for all PIN and command entries)*
- *Independent user & admin PINs*
- *Auto-lock feature (automatically locks when unplugged)*
- *Programmable brute-force protection*
- *Self-destruct PIN*
- *Forced Enrollment—eliminates the vulnerability of factory pre-set default PINs, AND enables the user to prove compliance with the GDPR requirement that the user changes the password on their device*

And without a doubt, companies absolutely should institute an organization-wide policy for secure use of USB drives with port control that manages device network access.

APRICORN

Methodology: Apricorn surveyed approximately 300 IT professionals from industries including education, financial services, government, healthcare services, legal, manufacturing, retail and manufacturing in Q4 2018. This survey was completed online, and responses were voluntary and completely anonymous.

apricorn.com