The State of USB Data Protection 2019 pt. II

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:

(6 out of 10)

organizations do not use port control / whitelisting software to manage USB device usage

(5 out of 10)

organizations require the deployment of encryption for data stored on USB devices

(9 out of 10)

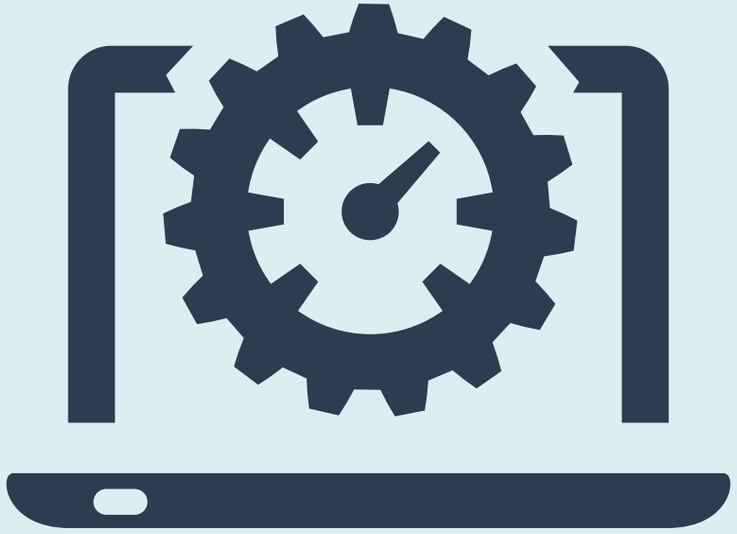
of these same organizations' employees believe that USB device encryption should be mandatory

This report – the second 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 pt. II



A Majority of IT Departments Are Failing to Implement the Necessary Tools to Manage USB Device Usage

As data breaches continue to become more frequent and damaging, companies need to closely monitor and analyze the data and information under the purview of the organization - including customer and partner data and information. The results of part I of this report confirm that most employees use USB drives, but are companies implementing the tools necessary to manage employees' USB drive usage?

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

58% of organizations do not use port control / whitelisting software to manage USB device usage

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

47% *of these same organizations require encryption for data stored on USB drives!*

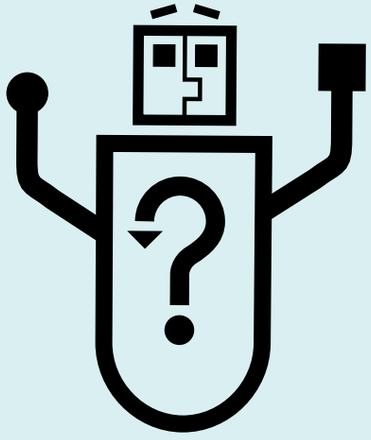
Takeaway:

Although USB drives are used by almost every employee, as we found in the Employee Spotlight report, employees begin ignoring security best practices as soon as they get their hands on a USB drive. As a result, it is incumbent upon IT departments to implement tools to help minimize the security risks associated with employees' USB drive usage. Yet as the above results illustrate, most IT teams are falling short in arming their organizations with these tools. The first step IT departments must take is ensuring - without fail - that when USB drives are deployed, they are encrypted.

The State of USB Data Protection 2019 pt. II

IT Departments' Policies for Secure USB Device Usage Are Severely Lacking

Considering that the vast majority of employees use USB drives, how comprehensive are organizations' existing policies for secure use of USB drives? By comparing the results in this report against Apricorn's 2017 State of USB Data Protection report, several trends emerge.



- **Less than half of organizations (47%) have a lost/stolen USB drive policy in place (compared to 50% in 2017.)**
- **The majority of respondents (53%) claimed their organization does not have appropriate technologies to prevent or detect the download of confidential data onto USB drives...**
- **But in Apricorn's 2017 survey, the majority of respondents (54%) claimed their organization DOES have those appropriate technologies.**
- **Nearly half of organizations (44%) do not have adequate governance and policies to manage the use of USB drives in the workplace (compared to 42% in 2017's report.)**
- **Less than half of organizations (47%) require the deployment of encryption for data stored on the USB drive (a slight improvement over 42% from 2017.)**
- **While more organizations in 2018 had a policy outlining acceptable use of USB devices than in 2017, more than one-third (36%) still don't have a policy in place.**

Takeaway:

While employees consistently acting against security best practices for USB drive usage is a significant concern, the larger issue is that employers aren't instituting policies to curb this behavior. IT departments have a wealth of opportunity to help their employees become more security-compliant users of USB drives, but IT teams are not only missing these opportunities, they are doing so at a higher rate than in previous years. It is crucial that employers educate their employees on the risks of not adhering to USB drive best practices - and that their IT departments enforce policy compliance.

The State of USB Data Protection 2019 pt. II

Conclusion: Given the increase in volume, sophistication and severity of security threats facing organizations today, it is critical that employers arm their employees with secure USB drives to prevent data breaches that lead to the loss of sensitive information. And this is especially true of organizations that regularly handle intellectual property and other highly confidential information. Considering 9 out of 10 employees use USB devices today, it is alarming that nearly 60 percent of employers fail to use port control or whitelisting software to manage USB device usage - and less than half of organizations don't require the deployment of encryption for data stored on USB drives.

The results of this report and the Employee Spotlight report are a wake-up call for organizations: it's time they asserted strict control over their employees' use of USB drives. As a result, employers should 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 fail, employers must institute organization-wide policies for the secure use of USB drives - with port control - to manage 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