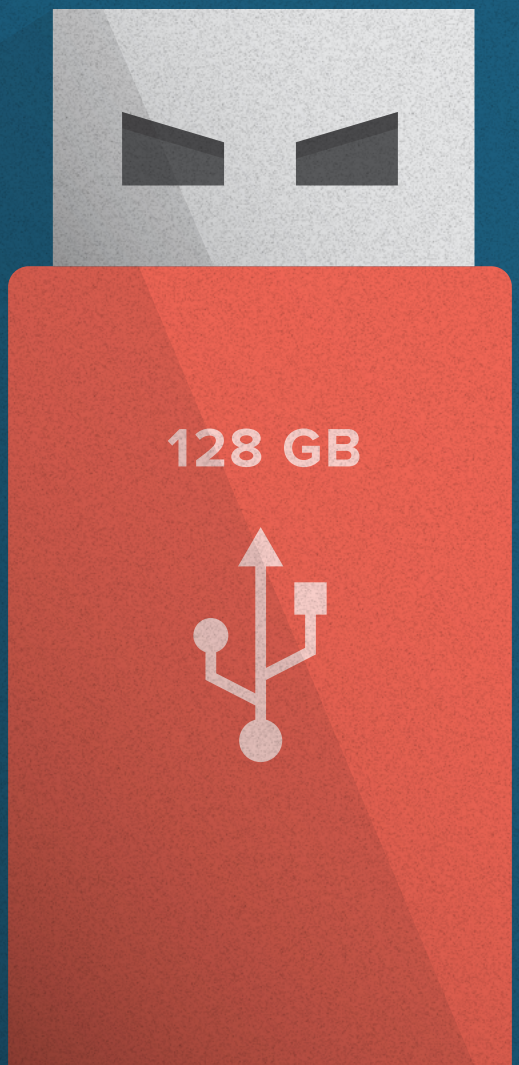
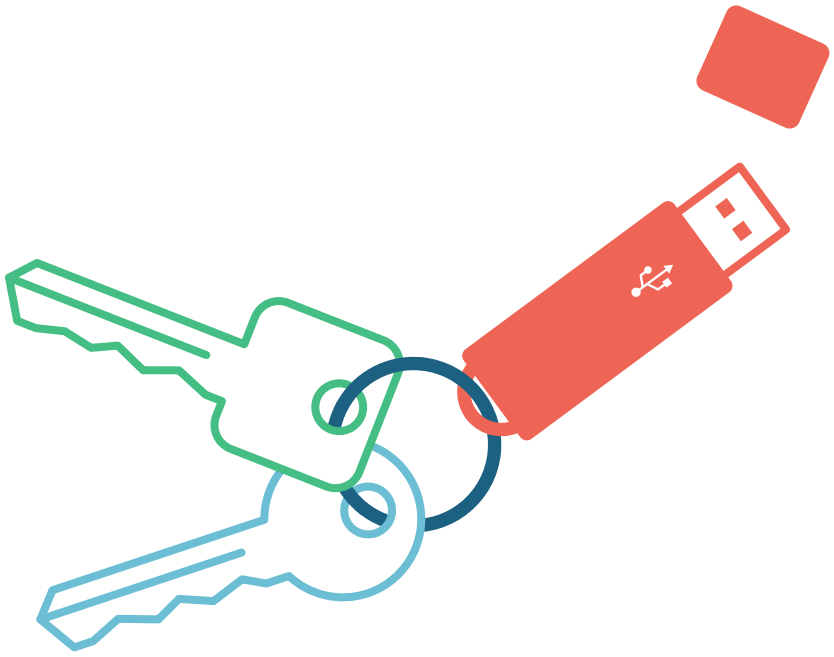
Neutralizing the USB Threat

Getting a handle on the slipperiest drives



Kingston TECHNOLOGY

Table of Contents



Introduction

Do USB drives pose a legitimate security threat to today's organizations? That depends. Do your employees and visitors who connect to your network ever use USB drives? Doesn't matter whether it's daily or only once in a blue moon, whether it's for work purposes or not, whether it's with your permission or not. If anyone's ever even thought about connecting a USB drive to your network, then your organization is at risk.

You can see how easily it could happen. It wasn't that long ago that IBM unknowingly gave out malware-ridden USB drives to attendees at a security conference in Australia.[1] Even the most security-conscious individual might be forgiven for plugging in an IBM-supplied USB drive without thinking twice.

And that's not the only possible scenario. What about the sales guy who has bought a cheap USB drive from the checkout display at his local electronics store? He may decide to bring his customer files home on the USB some Friday, rather than lugging his entire laptop. But then what if the drive falls out of his jacket pocket during happy hour after work? Or in the back of the Uber on the way home? Or on the golf course the next day? Drop that USB and it is gone forever—and the information on it is free for the taking. He has essentially taken a printout of the customer file and pinned it on a bulletin board.

So, yes, if there is a functioning USB drive in your building or on any device your users may access, then USB drives pose a security risk. That goes for organizations large and small, across all departments, across all industries, and across all geographies. What can we do about that? This paper looks at the threats USB drives pose and outlines specific options for addressing them.

Four Main Risks

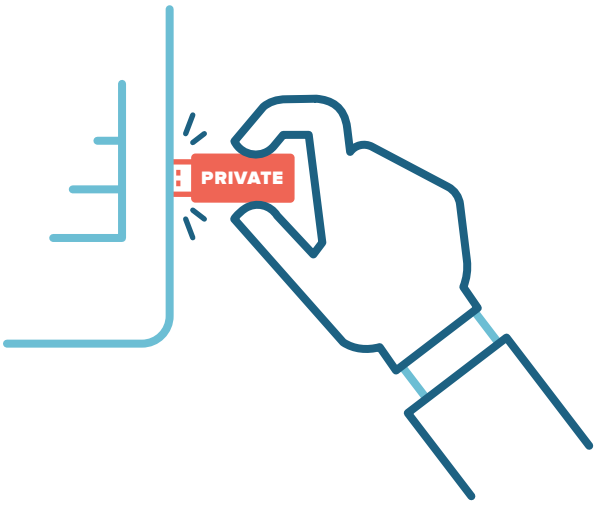
Theoretically, there are four main ways that a USB drive can pose a threat:

Someone in your organization accidentally loses a USB drive that's full of data.

Our fictional sales guy above is guilty of this, as are plenty of real-world employees. Do people really lose USB drives that often? Recent studies say yes. According to research conducted in the UK, more than 22,000 USB drives end up at the dry cleaners each year, left in their owners' pockets. Only about half of them are returned.[2]

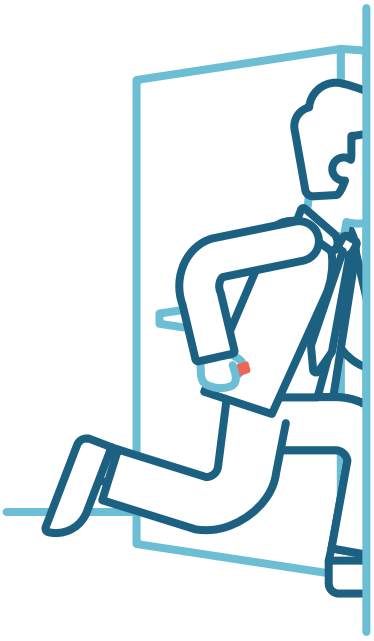
A USB drive that's full of data gets stolen from your organization.

You don't have to drop the USB drive in the parking lot in order to get into trouble. Sometimes the thieves come right to your door. In Indiana, an unencrypted USB drive storing data on more than 29,000 patients went missing straight out of a hospital emergency department.[3] An IT department at a life insurance company in Puerto Rico had a USB drive stolen that contained personal data for more than 2,200 people, including their names, dates of birth, and social security numbers. The theft was considered a violation of HIPAA compliance, and the company was fined a cool $2.2 million.[4]



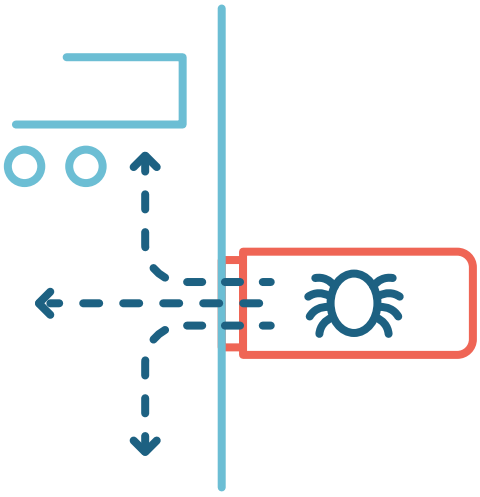
Some trusted but nefarious person in your organization absconds with data via USB drive.

This scenario makes for an all-too-common news item. It was recently reported that a disgruntled employee at the FDIC made off with a USB drive containing social security numbers and bank account information for approximately 30,000 people.[5] Likewise, a CalOptima employee who was leaving the company stole data on 56,000 patients via unencrypted USB drive.[6] The data included names and social security numbers, including those of children.



Someone in your organization finds an infected USB drive and plugs it in out of curiosity.

Maybe they found it in a parking lot, or maybe IBM gave it to them at a security conference. Either way, the problem is not merely an urban legend. A large-scale study conducted at the University of Illinois showed that 48% of people who find USB drives do plug them in and click on at least one file. Whether it's done out of curiosity or in a noble attempt to find the owner, the results to your network will be the same if the drive is infected with malware. The University of Illinois study, published in May 2016 at the 37th IEEE Security and Privacy Symposium, also showed that these events can take place very quickly. The first drive was connected in less than six minutes. Half of the drives were connected within seven hours.[7]



Are You Immune?

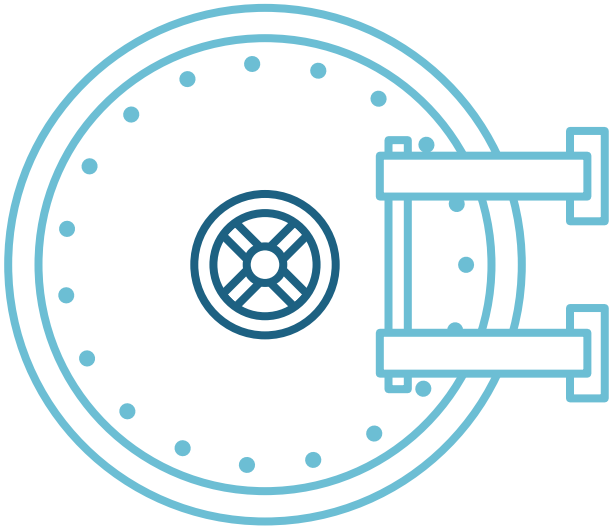
You don't have to be in financial services or healthcare to be concerned about the risks of USB drives. Lots of companies have valuable data, from account numbers and passwords to customer credit card information. Even a database of email addresses can be valuable to someone outside your organization. Whether it's stolen by a criminal or accidentally dropped at the bowling alley, losing any kind of company or customer data can be costly or otherwise damaging to your organization, no matter your size or your industry. Today's large-capacity USB drives make it even easier for people to lose (or steal) large amounts of data via USB.

In an attempt to curb this disturbing trend, regulations impacting USB security are starting to crop up. In 2016, the EU passed the General Data Protection Regulation, or GDPR, which is designed to strengthen data privacy for EU citizens. The hope is that GDPR will prevent the kind of data breaches that have plagued Europe for many years. For example, in 2015, a Bank of Barclay employee lost a USB drive containing sensitive data on 13,000 customers.[8] Likewise, the UK's Ministry of Defence reported that more than 100 USB drives containing restricted or secret data had been lost over a four-year period.[9]

...a Bank of Barclay employee lost a USB drive containing sensitive data on 13,000 customers.[8]

Once GDPR goes into effect in 2018, non-compliant organizations may face heavy fines. But GDPR will also impact organizations outside the EU that interact with EU companies. According to research conducted by Spiceworks, 38% of IT professionals say that GDPR will have an impact on their data protection practices—with many IT pros seeing it as a sign of things to come. In fact, 74% of respondents anticipate more national and/or international data security regulations in the next four to five years.

In the meantime, are IT pros worried about the potential harm USB drives can cause? Almost 30% of respondents reported that their employees use unencrypted USB drives, and 41% of respondents said they *were* concerned about the associated security risks. Almost 40% are worried specifically about lost or stolen drives, while 48% are worried about malware being introduced via USB drive. Even among those who keep a tighter lid on USB usage, 74% felt that unapproved or "shadow" use of USB drives still poses a threat to the organization.



What's an IT Pro to Do?

There are a handful of tactics IT pros can take—and have taken—in an attempt to mitigate the risks posed by USB drives. Of course, some tactics are more effective than others, and not all are appropriate for all organizations:

User Education

Education should always be the first line of defense, and explaining the different threat scenarios associated with USB drives may go a long way toward modifying bad USB behaviors. Education on USB use or any other topic is most effective when it's done on a regular basis, as opposed to a one-and-done approach. The feeling of urgency may fade over time, and best practices may slip the mind, so it's important to keep the topic fresh. Showing your users the parking-lot USB study, the dry-cleaner USB statistics, and recent news articles on USB security breaches may help drive the point home. According to the Spiceworks survey, only half of respondents currently educate their end users on the potential dangers of USB drives.

Restricted-Use Policies

Documented policies are an important part of the USB security strategy and should be communicated consistently. While 80% of survey respondents reported their organization has a specific policy regarding USB usage, 19% still allow their entire organization to use them. Just 30% limit usage to select use cases, while only 19% limit usage to encrypted USB drives. Ten percent ban the use of USB drives completely.

So, what are they concerned about? Regarding USB-related security threats, these IT pros were most concerned about infections (72%), data leaks/theft through an unencrypted drive (65%), and lost or stolen drives (64%). However, these concerns differ from actual experiences; of the 33% of organizations that have experienced USB-related security threats/breaches within the past year, the most common experience was lost or stolen USB drives.

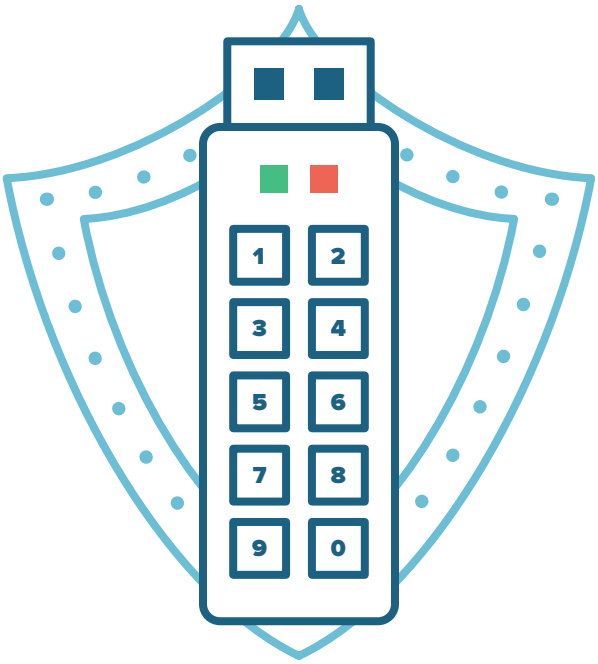
Policy Enforcement

Whether your policy bans the use of USB drives altogether or allows the use of USB drives only for certain departments, IT pros have better luck when they can enforce those policies using automated, systematic means rather than relying on the honor system or random inspections. For example, some organizations "whitelist" authorized or encrypted USB drives and run a USB kill utility when an unknown USB is connected. Other organizations disable or destroy USB slots entirely. Just be cognizant that if USB drives help your users get their work done, they may well figure out how to create a workaround for your enforcement mechanisms.

Encrypted USB Drives: A Powerful Weapon

When policies are too difficult to enforce but a full ban on USB drives is impractical, encrypted USB drives can be an ideal solution. For example, Kingston's IronKey USB devices offer XTS encryption and FIPS cryptographic certification. Whether the drives are lost or stolen, whether they are dropped at a restaurant or handed to a corporate spy, they won't give up their secrets. Unauthorized users can't simply plug them in and read the data.

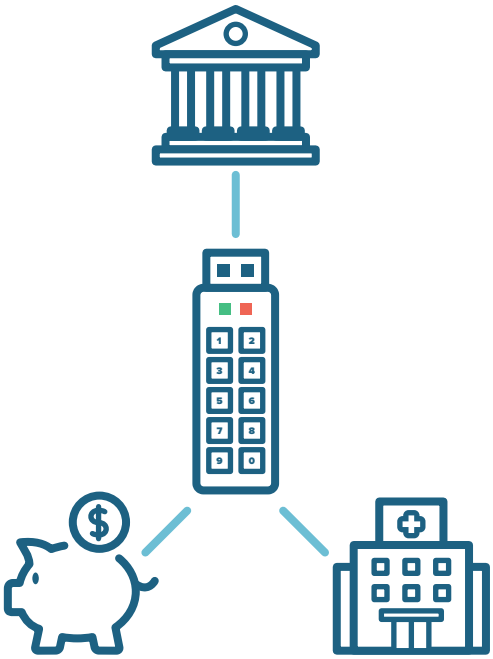
Today's encrypted drives come in a range of capacities and offer advanced management and security features, making them even more powerful against USB-related risks. For example, specific Kingston IronKey models offer anti-virus protection, complex password protection, and tamper-evident technology. Some models also have the ability to be managed remotely by management software that allows IT administrators to audit file activity, reset user passwords remotely, enforce policies, and even disable drives entirely, remotely locking them down in the event of loss or theft. Organizations can also use other types of management software to whitelist only encrypted drives, helping to prevent unauthorized devices from accessing the network. These advanced features of encrypted drives can help form a powerful barrier against USB-related security threats.



How Kingston Can Help

Kingston's IronKey line of encrypted USB 3.0 flash drives are used across government agencies, healthcare providers, financial companies, and organizations in many other industries to help meet stringent requirements for data security while allowing individuals and departments to do their jobs more efficiently.

In addition to advanced security features such as anti-virus protection and remote management capabilities, Kingston offers a secure customization program that provides encrypted drives, with popular options such as serial numbering, dual passwords, and custom logos.



Kingston TECHNOLOGY

ZONES
First Choice for IT™

For more information, contact your Zones account manager, or call 800.408.ZONES.

About the Spiceworks Survey

Kingston commissioned Spiceworks to conduct a survey in February 2017. The survey addressed IT decision-makers in the US, Canada, and Europe to capture existing policies, practices, perceptions, and experiences regarding USB drive usage and management. Results of the survey included responses from 300 participants from IT departments across multiple industries and in organizations of varying sizes.

Sources

[1] Andy Greenberg, "IBM Distributes Malware-Infected USB Sticks At Security Conference," *Forbes*, May 21, 2010. http://www.forbes.com/sites/firewall/2010/05/21/ibm-distributes-malware-infected-usb-sticks-at-security-conference/#6ea8bdc315d5

[2] Steve Bush, "22,000 USB sticks go to the dry cleaners," *ElectronicsWeekly.com*, January 14, 2016. http://www.electronicsweekly.com/news/business/information-technology/22000-usbs-sticks-go-to-the-dry-cleaners-2016-01/

[3] Taya Flores, "IU Health Arnett reports missing patient info," *JConline*, January 5, 2016. http://www.jconline.com/story/news/2016/01/05/iu-health-arnett-reports-missing-patient-info/78300400/

[4] Joseph Goedert, "HIPAA violations, stolen USB drive costs insurer $2.2M," *Health Data Management*, January 20, 2017. http://www.healthdatamanagement.com/news/hipaa-violations-stolen-usb-drive-costs-insurer-22m

[5] Tom Brant, "Report: FDIC Employees Caused Repeated Security Breaches," *PC Magazine*, July 15, 2016. http://www.pcmag.com/news/346179/report-fdic-employees-caused-repeated-security-breaches

[6] "Potential CalOptima PHI Data Breach Affects 56K Members," *Health IT Security*, October 20, 2016. http://healthitsecurity.com/news/potential-caloptima-phi-data-breach-affects-56k-members

[7] Elie Bursztein, "Concerns about USB security are real: 48% of people do plug-in USB drives found in parking lots," *Elie.net*, April 2016. https://www.elie.net/blog/security/concerns-about-usb-security-are-real-48-percent-of-people-do-plug-in-usb-drives-found-in-parking-lots

[8] "Fraudsters had access to 13,000 Barclays customers' sensitive data 'for seven years'," *The Telegraph*, July 24, 2015. http://www.telegraph.co.uk/news/uknews/crime/11762339/Fraudsters-had-access-to-13000-Barclays-customers-sensitive-data-for-seven-years.html

[9] "MoD admits loss of secret files," *BBC*, July 18, 2008. http://news.bbc.co.uk/2/hi/uk/7514281.stm