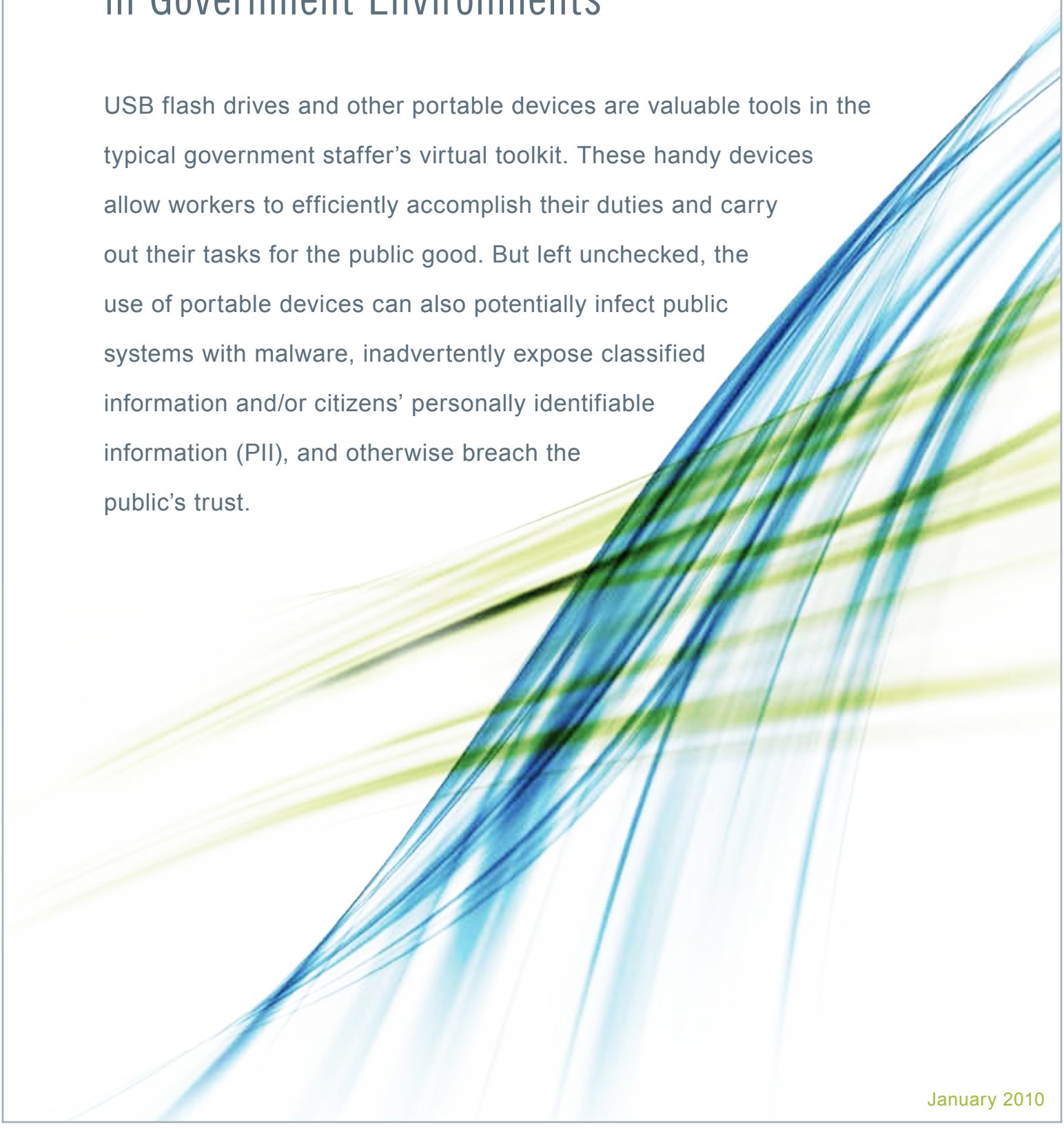
The Great Balancing Act: Using USB Flash Drives in Government Environments

USB flash drives and other portable devices are valuable tools in the typical government staffer's virtual toolkit. These handy devices allow workers to efficiently accomplish their duties and carry out their tasks for the public good. But left unchecked, the use of portable devices can also potentially infect public systems with malware, inadvertently expose classified information and/or citizens' personally identifiable information (PII), and otherwise breach the public's trust.



January 2010

WP-EN-01-08-10

Overview

From the establishment of the USB 1.0 standard to the rollout of iPods and thumb drives, and all the way through the development of USB 3.0-enabled mega-storage devices, portable device innovation has always been about speed, capacity and convenience. This has meant great things to the public sector, which leverages these devices for incredible productivity gains. For example, workers can now use ultra-portable flash drives to easily transfer large amounts of data within highly distributed environments. They can use these same devices to store important presentation information while on the road at conferences and briefings. For military personnel in the field, these devices are used to quickly transfer data.

Unfortunately, many of these gains could well be wiped out for government entities if these devices end up enabling a catastrophic data breach. Even as USB devices have evolved into useful storage media, they've also turned into a security nightmare for agencies.

It's apparent to anyone who reads the news regularly that USB devices are involved time and time again in some of today's highest-profile data breaches, either through the loading of breach-causing malware onto the network, by facilitating intentional covert removal of sensitive data, or simply by enabling data loss through the loss of an unencrypted device.

And it's not just USB devices that are a threat, either. In fact, they're just the tip of the iceberg. All of the same threats also extend to all forms of removable media in use today including CD, DVD and Blu-ray drives as well as FireWire- and eSATA-connected devices.

Clearly, the real key to the successful use of all portable devices is striking the right balance between the productivity they offer and the risks they pose.

The Utility of USB Devices

Once a mere novelty peripheral, USB storage devices are now about as common now as the mouse and keyboard. According to analysts with In-Stat, more than 3 billion USB devices shipped in 2008 alone, and those numbers will only keep ticking upward. In-Stat estimates a 6.6 percent compound annual growth rate for these devices through 2013.

Portable devices have increasingly become a staple of the office environment, whether an organization provides them for workers or not. A recent survey conducted by Applied Research-West on behalf of SanDisk found that 77 percent of corporate users say they have used a personal flash memory device for work purposes. (Presumably this is similar to what is seen in government organizations.) And that's not counting the use of other devices such as iPods, cameras and smartphones that workers commonly plug into their workstations for personal use as well. The fact is that USB devices are ubiquitous within most environments.

And what's more, most users don't understand the risks they take when they use these devices on the agency infrastructure. For example, one in 10 workers surveyed by Applied Research reported having found flash drives in public places. Of those, more than half admitted that one of the first things they would do is plug in the foreign device to find out what was on it—a risky proposition, given the amount of malware that can be downloaded upon connection with an endpoint.

While many IT managers do recognize what kind of problems such end user mistakes can promote, the knee-jerk reaction to enact an outright ban of USB devices and other portable media is hardly an effective strategy. One need only look to the U.S. Department of Defense (DOD) to see how truly impractical this strategy is.

DOD: A Case Study in Refining Draconian Policy

In the fall of 2008, DOD brass got a first-hand look at how risky unfettered use of USB memory sticks can really be. It was around that time that signs started popping up in the SIPRNet (and the less sensitive NIPRNet) that this extremely sensitive and classified network had been infected by a Trojan.

As officials investigated, they found the culprit was SillyFDC, a relatively harmless worm that nevertheless gave military officials quite a scare by its unauthorized presence on such sensitive systems. This sneaky piece of malware managed to worm its way onto supposedly iron-tight systems through—you guessed it—infected USB memory sticks.

The reaction to the SillyFDC attack was as swift as it was resolute. In November 2008, the DOD announced a complete ban on USB storage devices, flash memory cards, PDAs and portable music players.

Problem was, the moment the ban was enacted, civilian and military branches of the DOD immediately began banging up against a host of operational difficulties. Throughout late 2008 and most of 2009, personnel complaints made it clear that USB devices in many cases weren't tools of convenience, but rather of utmost necessity.

According to an October 2009 article in Defense News, prior to the ban many military aircraft and vehicle technicians were using thumb drives to store once-hefty technical manuals. Medical personnel were taking advantage of them to ferry medical records of wounded troops from field hospitals in Iraq to Germany and the United States. Pilots used them to transfer mission plans from operations rooms to aircraft computers. And countless more personnel used them to easily transport photos, briefings, presentations and other documents between meetings and scattered locations.

All of this important activity was put to a stop in favor of accessing material from firewalled and protected network assets. Unfortunately, in the military's highly distributed and sometimes unconnected world, network access was often simply impossible.

> And so, in October 2009, the DOD announced it was relenting on its draconian policy. Rather than restrict outright the use of USB devices, the DOD is now bringing back the USB drive—this time in a much more controlled fashion. The DOD now limits who can use the devices and only allows authorized and secured devices to connect to DOD assets.
>
> "The bottom line is, the days of using personally owned flash media or using flash media collected at conferences or trade shows are long gone. What we connect to our home PCs is very different from what is and will be allowed to occur on DON networks," Robert Carey, chief information officer for the Department of the Navy, wrote in his blog on the matter. "I expect (and support) that only approved, identifiable flash media of known origin will be permitted for use; and only by authorized and trained personnel, in support of mission-essential functions that could not be performed via non-flash media means."

In a recent opinion piece on the USB policies, Gartner analyst Neil MacDonald explained that blanket bans are ineffective.

"This may indeed be necessary and provides immediate protection of data loss. However, it's a blunt, coarse control that really doesn't solve the underlying problem," he wrote. "Such drastic policies get in the way of legitimate users trying to do their job. Better, how about a control that enforces a policy like 'don't allow sensitive data to be copied to a USB drive unless the data (or the drive itself) is encrypted.'"

The recent move by the DOD to reinstitute the managed use of USB devices shows that government entities are coming around to MacDonald's line of thinking in terms of finding the right balance of productivity and risk.

Surveying the Risks

Simply put, the ease of use, the prevalence of the format and the inherent insecurity of USB make it a dream for most cybercriminals and cyberterrorists. Not only that, but the small size and portability that make these devices so useful also make them as easy to lose as a kid's coat on a schoolyard. To determine a way to take advantage of portable devices without risking too much in the process, it is important to first thoroughly understand the threats that will need to be addressed. Let's examine three of the top risks.

1. Data Loss

By far the most common way a typical employee will expose his or her organization to risk through USB use is simply by misplacing a device containing sensitive data. It is all too easy to accidentally leave behind a portable device on public, unsecured computers, such as those in hotel business centers. It happens all of the time. In fact, The Ponemon Institute estimates that 800,000 data-sensitive devices—including USB drives, hard drives, laptops and mobile devices—are lost or stolen each year.

A glaring example of such a loss happened in April 2009 at the National Archives and Records Administration (NARA) when an employee lost an external hard drive containing more than 1TB of information with details about "100,000 Clinton administration officials, Secret Service and White House operating procedures, event logs, social gathering logs, political records and other highly sensitive information," according to NARA's report to Congress.

This could this pose a danger to sensitive government information. And make no mistake, government employees are using these devices to store very important data. In June 2009, the Ponemon Institute released statistics that said that 69 percent of surveyed employees copy confidential or sensitive business information onto USB devices. (Presumably this is similar to what is seen in government organizations, which typically do not publish this kind of data.) Of those surveyed, only 13 percent said their organizations have a policy allowing the practice, meaning that even blanket bans don't mean much without enforceable controls.

2. Data Theft

The unchecked use of portable devices within an organization can also open it up to the risk of massive data theft through storage that only keeps growing in capacity—today's common flash drives are pushing past 100GB, and larger external hard drives of 5TB or more can easily be picked up by workers at the local big box retailer.

That voluminous capacity alone can make these devices a prime virtual cybercriminal's bag to run away with the agency jewels. When paired with certain sinister software tools, these devices can be used to even more devastating effect. One of the first programs to really highlight the threats posed by USB usage, Pod-Slurp, is a great example of such a tool. Simply plugging a USB device loaded with Slurp into a victim's computer would automatically start the scripts copying each and every document from the host PC's My Documents directory onto the USB stick. One could modify the script to target spreadsheets, PowerPoint files or any specific file type of one's choice. Further, it could easily be modified to send files via e-mail or FTP instead of copying them to the USB device.

Considering the growing stormfront of cyberwarfare facing the U.S. from state and non-state actors, the threat of theft through USB data dumps is a clear and present danger. Be they state secrets, sensitive infrastructure schematics and details, or military plans, there are a multitude of data stores ripe for theft by spies and other nefarious people trolling for information at every government level.

Continued »

3. Malware Propagation and Hacking

It is not only legitimate users who enjoy the benefits of today's USB devices. Cybercriminals are increasingly using removable media to introduce malware into computers.

Security companies are reporting an increase in malware that propagates via USB devices and other removable media. Malware, such as the SillyFDC worm that plagued the Army in 2008, the many variants of viruses that cropped up to exploit Microsoft Autorun vulnerabilities in 2009 and several variants of Conficker, copy themselves to all drives connected to infected machines. Any USB device connected to an infected machine then becomes infected, and later when it is connected to yet another machine, that machine too also begins infecting other USB devices plugged into it. This "worm-like" malware propagation method copies itself to all available drives, shares, removable media and peer-to-peer software application file folders.

This can greatly increase the exposure of an organization that may otherwise have its network security bases covered. One infected endpoint can easily spread malware to a shared USB stick, which then can further infect any other endpoint to which it connects.

In addition to propagating malware, USB drives can also prove to be an exceptional hacking platform for those attackers with physical contact to agency machines. One of the many legitimate, useful features of USB drives is their ability to act as a "PC on a stick" through the use of certain platform and virtualization utilities, such as BartPE/PeToUSB, UBCD4, UNetBootin and MojoPac. But again, this legitimate use can also be used for dark purposes. It also makes it possible for malicious users to replicate their entire Windows hacking lab with a USB device and run it on virtually any PC with an available USB port. When the malicious user is done, she simply removes the USB device and leaves without a trace.

Reaping Productivity Gains without the Risks

The traditional definition of an "endpoint" is clearly evolving. For millions of users, portable mass media represents the next generation of endpoints, shifting from simply PCs and laptops. Because of this evolution, agency endpoint security must also grow to address the increasing concerns. Ultimately, this shifting endpoint exposes a new threat vector that IT professionals must confront and secure. As Gartner's MacDonald points out, using epoxy to block USB ports is not the answer. Clearly the productivity gains brought by the many USB devices available today outweigh the safety of a total ban. In fact, given the state of today's economy, the use of USB devices should be encouraged and embraced to help reduce operating costs and improve productivity.

Lumension® Data Protection enables organizations to develop and enforce granular usage policies for removable devices (such as USB flash drives) and other removable media (such as CDs and DVDs) to control the flow of data to and from your endpoints—working with the devices rather than simply enabling or disabling them. The products that comprise Lumension Data Protection include:

- *Lumension*® Device Control, which enforces organization-wide usage policies for removable devices, removable media and data (such as read/write, encryption).
- Lumension® Device Control for Microsoft® System Center, which seamlessly integrates the capabilities of Lumension Device Control into an already-established SCCM environment to reduce implementation costs and quickly enhance security policy enforcement.

Removable devices are validated as they are used within the organization. Devices that are not explicitly authorized are simply not allowed to run. Through a central console, device control policies are quickly established and enforced through two simple steps: identification and assignment.

Policies are managed per user or user group as well as per computer. For devices, policies are enforced by file type (particularly useful in preventing executables such as malware from being downloaded onto your network), daily volumes, time of day and many more criteria. Lumension Data Protection enables the immediate association of user groups to devices on the fly—dramatically simplifying the management of endpoint device resources.

Lumension Data Protection can also force encryption of removable media so that it can be safely used and transported without the fear of exposing confidential data to unauthorized users. Users can access their data on any computer on the network, or they could be also allowed to access their encrypted data even on computers that do not have client software installed. Centralized and decentralized encryption schemas provide the administrator with the flexibility to centrally encrypt removable media or enable users to encrypt removable media on their own and, more importantly, enforce the use of that encrypted media.

In certain situations, administrators might want or need to enable trusted users to authorize their own devices, but still have visibility and be able to audit these users' activity. Auditing and reporting functions enable administrators to precisely track when devices are used, by whom and how—and even retain a copy of any data being written to a removable storage device. They can also see attempts to use unauthorized devices and track that as well.

Engaging in the USB Balancing Act

To win the war against mobile malware and information theft, organizations must develop clear, in-depth policies regarding the use of removable devices and media. They must also deploy proactive approaches, such as the Lumension Data Protection solution, to support and enforce these policies. After all, the notion of a "PC on a stick" should benefit the day-to-day process of government workers, not impede them.

About Lumension Security, Inc.

Lumension Security, Inc., a global leader in operational endpoint management and security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets. Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, and Compliance and Risk Management offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year. Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Virginia, Utah, Florida, Texas, Luxembourg, the United Kingdom, Germany, Ireland, Spain, France, Australia, and Singapore. Lumension: IT Secured. Success Optimized.™ More information can be found at www.lumension.com.

Lumension®
IT Secured. Success Optimized.™

Global Headquarters
8660 East Hartford Drive, Suite 300
Scottsdale, AZ 85255 USA
phone: +1.888.725.7828
fax: +1.480.970.6323