Ponemon INSTITUTE

The State of USB Drive Security in the United Kingdom

Sponsored by Kingston Technology

Independently conducted by Ponemon Institute LLC

Publication Date: November 2011

The State of USB Drive Security in the United Kingdom

Ponemon Institute, November 2011

Introduction

Sponsored by Kingston Technology, Ponemon Institute is pleased to present the results of *The State of USB Drive Security in the United Kingdom.* The focus of this research is to better understand how complex business and government organizations manage the security and privacy requirements of data collected and retained on USB drives.

We believe the lesson to be learned from the research is that organizations do understand they are at risk because of employees' negligence but are often not taking the necessary steps to secure USB drives. Our study also reveals that while these devices may be small, the data breaches that can result from lost or stolen USBs are huge. Approximately 72 percent of respondents say that a data breach was caused by sensitive or confidential information contained on a missing USB drive.

The following are 10 USB security practices that many organizations in this study do not practice:

1. Providing employees with approved, quality USB drives for use in the workplace.
2. Creating policies and training programs that define acceptable and unacceptable uses of USB drives.
3. Making sure employees who have access to sensitive and confidential data only use secure USB drives.
4. Determining USB drive reliability and integrity before purchase by confirming compliance with leading security standards and ensuring that there is no malicious code on these tools.
5. Deploying encryption for data stored on the USB drive.
6. Monitoring and tracking USB drives as part of asset management procedures.
7. Scanning devices for virus or malware infections.
8. Using passwords or locks.
9. Encrypting sensitive data on USB drives.
10. Deploying procedures to recover lost USB drives.

We surveyed 451 IT practitioners in UK with an average of 9.73 years of IT or IT security experience. Most of the respondents (58 percent) report to the chief information officer and 66 percent are at the supervisor level or higher in their organizations. Sixty-five percent of these respondents acknowledge it is very important or important that USB drives meet high data security standards.

The next section reports the key findings of our independently conducted survey research. Taken together, our results provide strong evidence that organizations are not addressing the potential data protection and security risks caused by the rash of ubiquitous and unsafe USB drives that are prevalent in many organizations. Please note that in many of the survey questions more than one response was allowed. As a result, the response frequencies shown in the key findings may total more than 100 percent.

Key Findings

The risk of unencrypted USB drives is ignored. In general, respondents seem to be pessimistic about the actions their organizations are taking to protect sensitive and confidential information on USB drives. Although 65 percent of IT practitioners in this study understand the importance of high data security standards for USB drives, 39 percent agree that their organizations make the protection of confidential and sensitive information collected and temporarily stored on these devices a high priority.

As further evidence of the lack of priority, only 32 percent of respondents say their organizations have governance procedures, controls and policies to stop or curtail employees' misuse of USB drives in the workplace. Even more serious is that only 29 percent say they have the appropriate technologies to prevent or detect virus or malware infections that may reside on USB drives before use by employees in the workplace.

Employees are negligent when using USB drives and this is putting organizations' sensitive data at risk. Employees are doing the following all the time or very frequently: using USB drives without obtaining advance permission to do so (73 percent) or losing USB drives without notifying appropriate authorities about this incident (72 percent). However, less than half (40 percent) of respondents say their organizations provide employees with approved USB drives for use in the workplace. Instead, 55 percent say employees are using generic USB drives that are received "free" at conferences, trade shows and other events.

More organizations should have enforceable policies that define the acceptable use of USB drives and enforce those policies. Fifty percent of respondents say their organizations have USB security policies. Of those organizations that have policies, 43 percent say they require employees who have access to sensitive and confidential data to only use secure USB drives. However, less than half (48 percent) of respondents say their organizations do not enforce compliance with policies primarily because they are relying upon the integrity of their employees (60 percent) or they do not want to hinder their productivity (55 percent).

Organizations use similar criteria for the selection of USBs as they do for other memory or storage technologies. The top three criteria for purchasing USB drives and other memory storage devices are: price, security certification and testing and the ability to prevent such attacks as malware, botnets and viruses. To assess the reliability and integrity of USB drives, 50 percent of organizations only purchase from trusted vendors followed by 45 percent of respondents who say their organizations confirm compliance with leading security standards. To keep low quality USBs out of the hands of their employees, 50 percent say their organizations create a policy followed by 43 percent who say their organizations do nothing.

USB drives are prevalent in an organization and most are not secure. Based on the findings there are, on average, 49,397 USB drives used by employees in the organizations represented in this study. On average, respondents believe less than half (46 percent) of these devices are secure. The most common types of sensitive or confidential information on an USB drive are: customer data and non-financial confidential documents.

The devices may be small but the data breaches as a result of missing USBs can be devastating. The vast majority of respondents (72 percent) in this study say that they are absolutely certain (31 percent) or believe that it was most likely (42 percent) that a data breach was caused by sensitive or confidential information contained on a missing USB drive. In the past 24 months, an average of 4.6 separate incidents involving the loss of sensitive or confidential information contained on a missing USB drive occurred in the organizations in this study. Thirty-seven percent of respondents believe with absolute certainty or likelihood that these drives contained customer, consumer or employee data.

End-user negligence as opposed to maliciousness is most often the cause of missing USB drives. On average**,** 67 percent of all missing USB drives are caused by negligence rather than fraud, theft or other malicious acts. Based on this finding, training and awareness programs and policies should be the first steps organizations take to improve the state of USB security.

Conclusion

USB drives have become an indispensable technology for employees in all organizations. However, as shown in this study, lost or stolen USB drives pose great risks to an organization's most sensitive and confidential information. While organizations seem to understand the need to become more proactive in making sure employees are not negligent, USB security practices do not seem to be a part of their overall data protection strategy.

In our introduction to this report, we listed 10 USB security practices that organizations should practice but many do not. Unfortunately, the study shows that this may be a challenge for IT and IT security practitioners because only 39 percent agree that their organizations view the protection of confidential and sensitive information collected and temporarily stored on USB drives as a high priority.

Our goal in presenting this research is to show that USBs may look insignificant but the consequences of a data breach from a lost or stolen device can be huge. More than 72 percent of respondents in this study say they are absolutely certain or believe it was most likely that a data breach their organizations experienced was the result of sensitive or confidential information contained on a missing USB drive.

On average, in the past 24 months organizations in our study have lost more than 17,000 records about customers, consumers and employees contained on USB drives. Based on Ponemon Institute's *2010 Annual Cost of a Data Breach Study*, the financial consequences of having a data breach as a result of lost or stolen records can be significant. According to our research, the average cost per lost or stolen record in the United Kingdom is £71We believe this staggering amount makes a convincing case of the need to introduce policies, procedures and training programs to mitigate the potential for a USB data breach.