Ponemon INSTITUTE

The State of USB Drive Security

U.S. survey of IT and IT security practitioners

Sponsored by Kingston

Independently conducted by Ponemon Institute LLC

Publication Date: July 2011

The State of USB Drive Security

US Study of IT & IT Security Practitioners

Ponemon Institute, July 2011

Introduction

Sponsored by Kingston, Ponemon Institute is pleased to present the results of *The State of USB Drive Security.* 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 not taking the necessary steps to secure USB drives. The main reasons cited for not being proactive include: uncertainty about monitoring and tracking USB use in the workplace, desire not to diminish productivity and the reliance on employee integrity and trustworthiness.

Our study also reveals that while these devices may be small, the data breaches that can result from lost or stolen USBs are huge. More than 70 percent of respondents in this study say that they are absolutely certain (47 percent) or believe that it was most likely (23 percent) that a data breach was caused by sensitive or confidential information contained on a missing USB drive. On average organizations in our study have lost more than 12,000 records about customers, consumers and employees as a result of missing USBs.

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

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

We surveyed 743 IT and IT security practitioners with an average of 10 years of relevant experience. Most of the respondents report through the IT organization (CIO) or to the organization's information security leader. The majority of respondents acknowledge the importance of USB drive security in meeting data protection and business objectives.

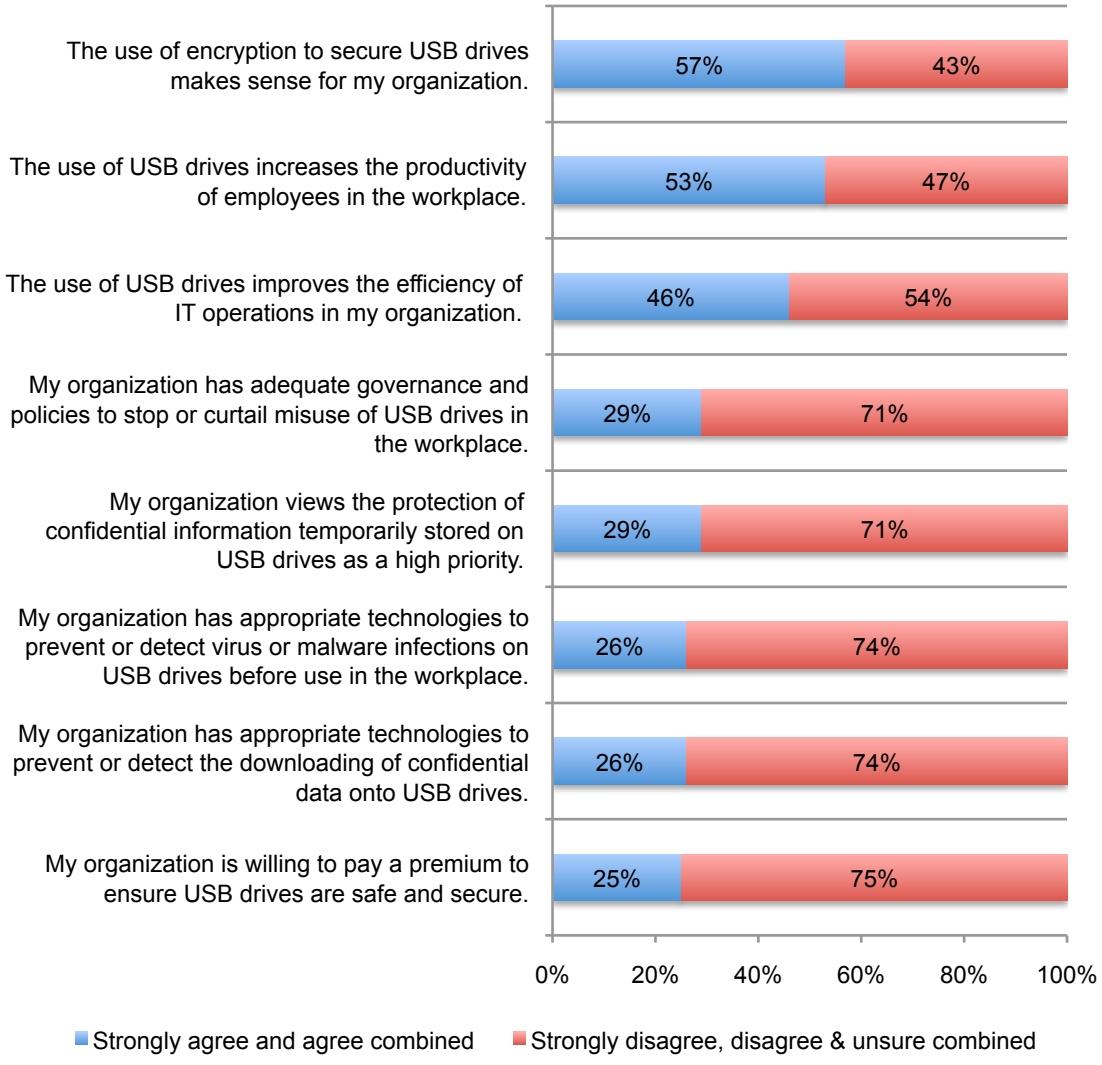
The next section reports the key findings of our independently conducted survey research. Taken together, our results provide strong evidence that organizations are not addressing the potential data protection and security risks caused by the rash of ubiquitous and unsafe USB drives that pervade many organizations.

Part 2. Key Findings

Organizations are ignoring the risk of unencrypted USB drives. Bar Chart 1 reports eight statements about the use and security of USB drives in respondents' organizations. Each statement or "attribution" is rated by respondents using a five-point scale from strongly agree to strongly disagree. To simplify results, we consolidate responses into two groups – namely favorable (strongly agree and agree responses) and unfavorable (strongly disagree, disagree and unsure responses).

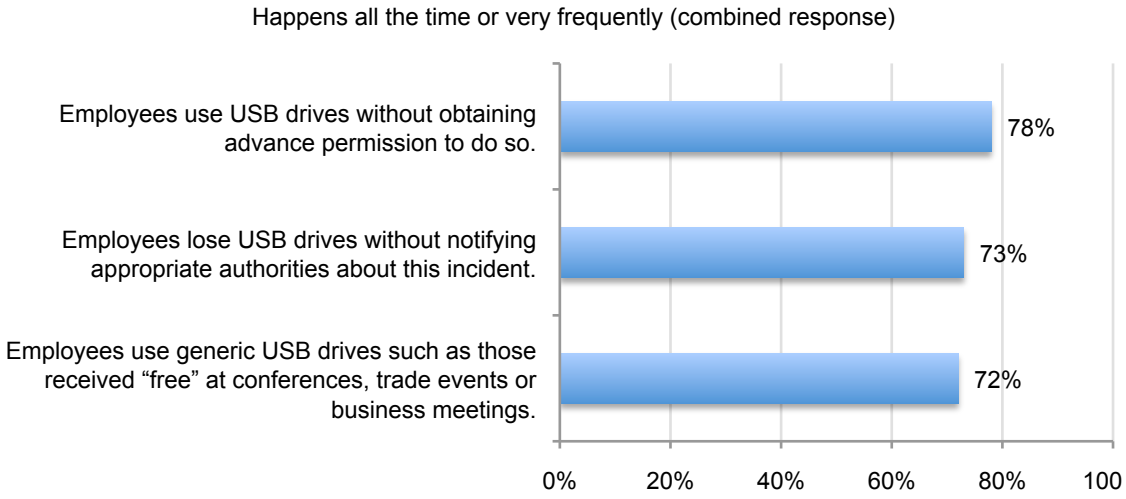
Seventy-one percent of respondents do not believe that their organizations consider the protection of confidential and sensitive information collected and temporarily stored on USB drives as a high priority. This is evidenced by the belief of 74 percent of respondents who say their organizations do not have the appropriate technologies to prevent or quickly detect the downloading of confidential data onto USB drives by unauthorized parties. The same percentage also say their organization does not have appropriate technologies to prevent or quickly detect virus or malware infections that may reside on USB drives before use by employees in the workplace.

Bar Chart 1: Attributions about the use and protection of USB drives in the workplace



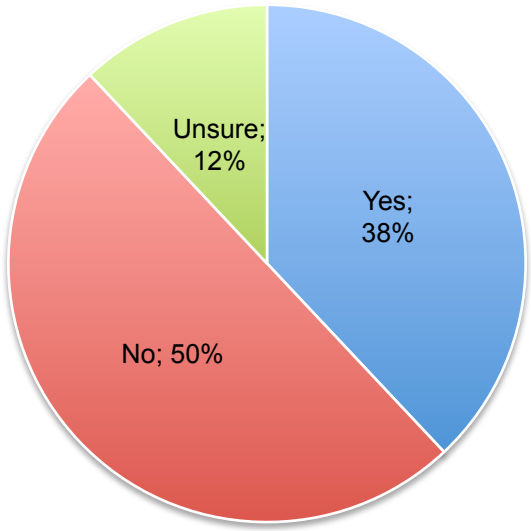
Employees are negligent when using USB drives and this is putting organizations' sensitive data at risk. Employees are doing the following: using USB drives without obtaining advance permission to do so all the time (50 percent) and frequently (28 percent); lose USB drives without notifying appropriate authorities about this incident all the time (49 percent) or very frequent (24 percent) and use generic USB drives such as those received free at conferences, trade events and business meetings all the time (52 percent) and frequently (20 percent).

Bar Chart 2: How frequently do the following scenarios occur?

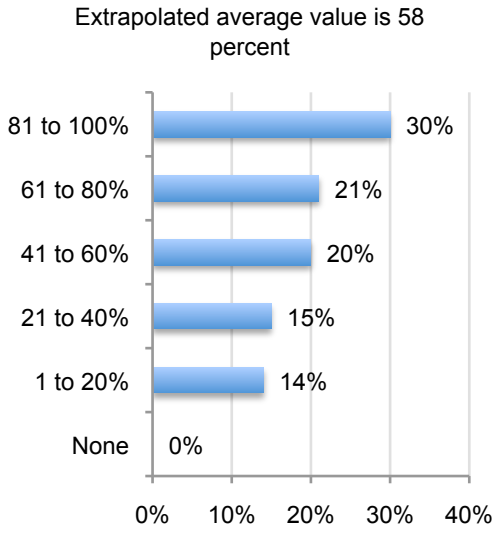


Despite awareness of employees' abuse of USB drives, the vast majority of respondents (75 percent) say their organizations are not willing to pay a premium to ensure USB drives used by employees are safe and secure (not shown in the chart). In fact, as presented in Pie Chart 1, half of respondents say their organizations do not provide employees with approved USB drives and 12 percent are unsure. While 38 percent of respondents' organizations supposedly provide approved USB drives to employees, an extrapolated average of 58 percent of employees in these organizations continue to use unapproved USB drives (see Bar Chart 3).

Pie Chart 1: Does your organization provide employees with an approved USB drive for use in the workplace?

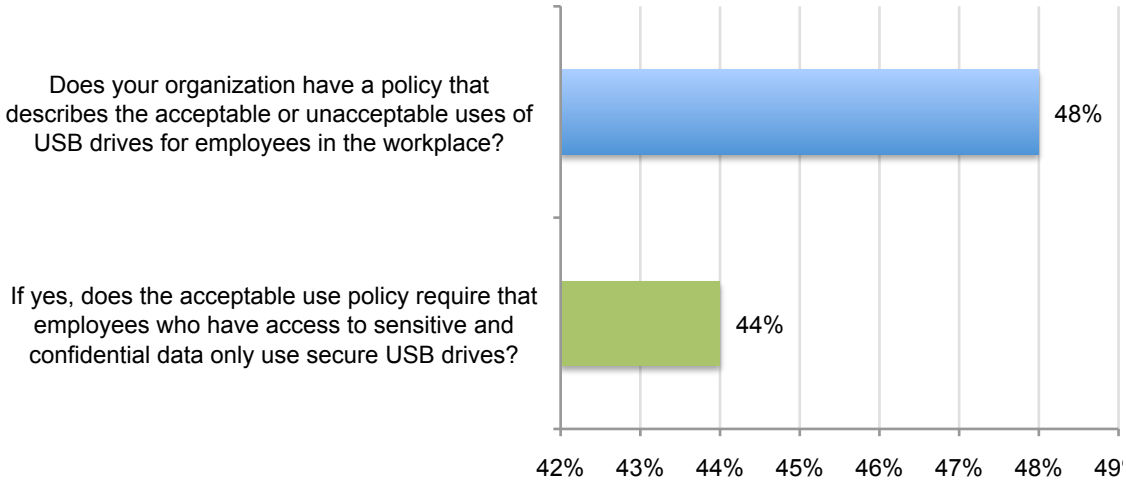


Bar Chart 3. If yes, despite availability of approved USB drives, what percentage of employees use unapproved USB drives in the workplace?



Organizations could improve the state of USB security by having policies that define the acceptable use of USB drives and enforcing those policies. As shown in Bar Chart 4, less than half (48 percent) of respondents say their organizations have USB security policies that define acceptable use.

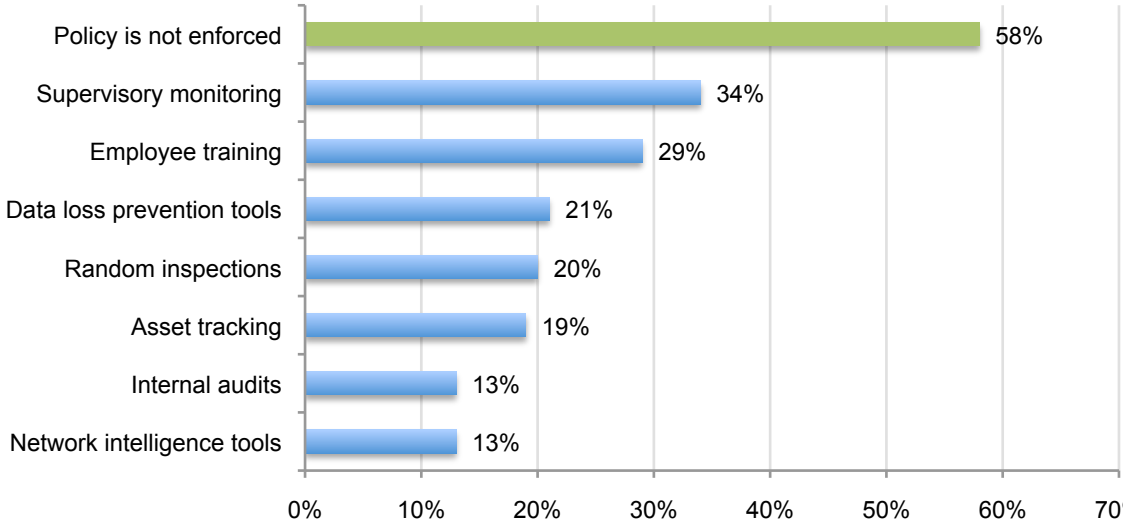
Bar Chart 4: Do organizations have a policy that defines the acceptable use of USB drives



Of those organizations that have policies, 44 percent say they require employees who have access to sensitive and confidential data to only use company-approved or secure USB drives. While not shown in the chart, 39 percent say their organizations do not require this and 17 percent are unsure.

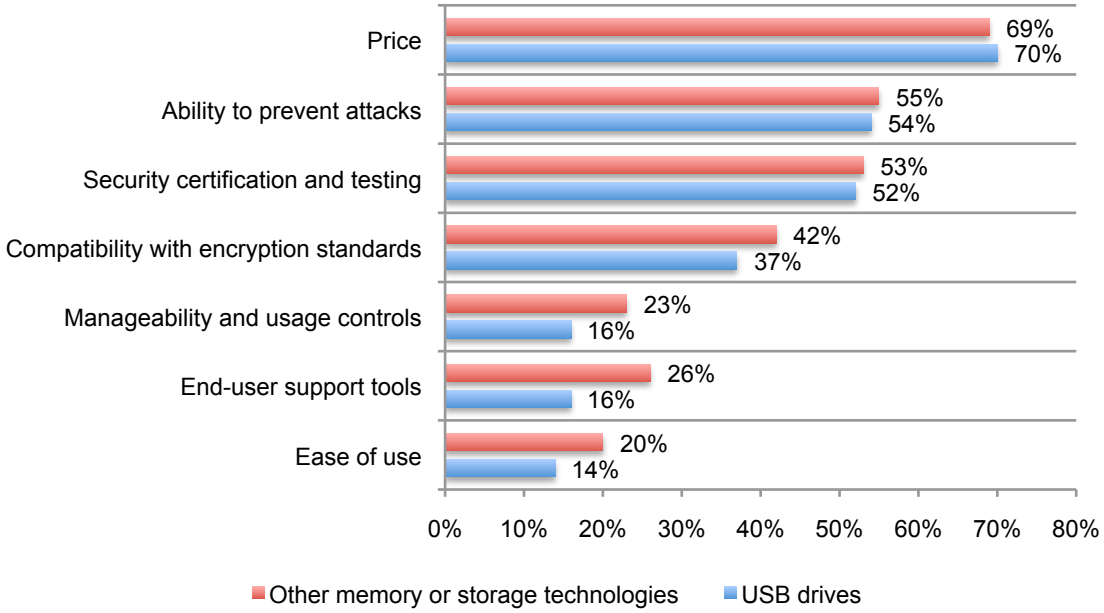
Bar Chart 5 summarizes how compliance is enforced. In many cases, acceptable use policies are really meaningless because 58 percent say they do not enforce compliance followed by 34 percent who say they enforce compliance through supervisory monitoring and 29 percent who say they enforce compliance through employee training. The top two reasons for not enforcing these policies are that they do not have the tools or resources to monitor compliance and the desire not to hinder employee productivity.

Bar Chart 5: How do organizations enforce their USB acceptable use policies?



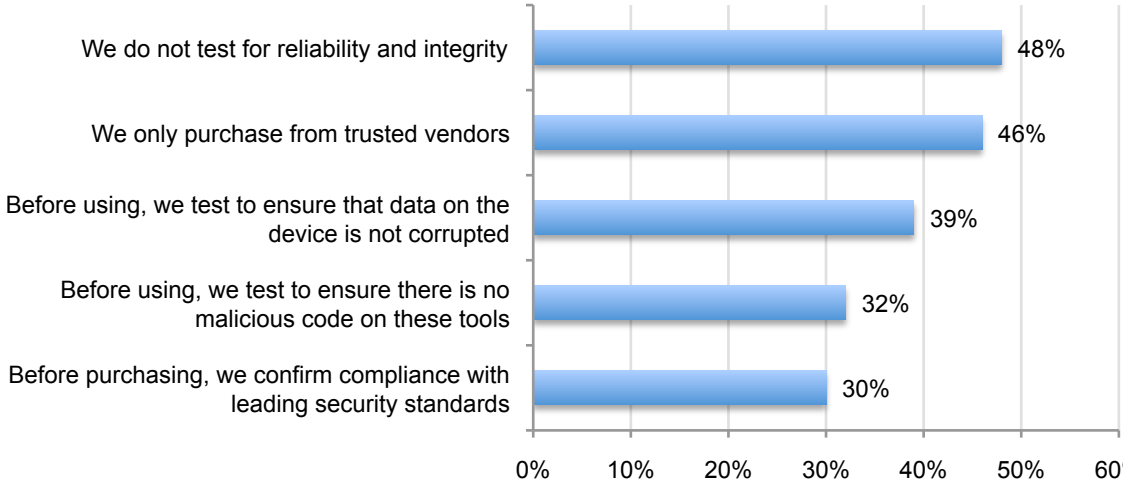
Organizations use the same criteria for the selection of USBs as they do for other memory or storage technologies. This comparison is shown in Bar Chart 6. As reported, price; the ability to prevent malware, botnets and viruses; and security certification and testing are the top three criteria most important for the purchase of USB drives. Despite concern about not diminishing productivity, end-user support tools and ease of use are not as important for USB drives as for other memory or storage technologies.

Bar Chart 6: What criteria are most important for organizations when purchasing USB drives and other memory or storage technologies?



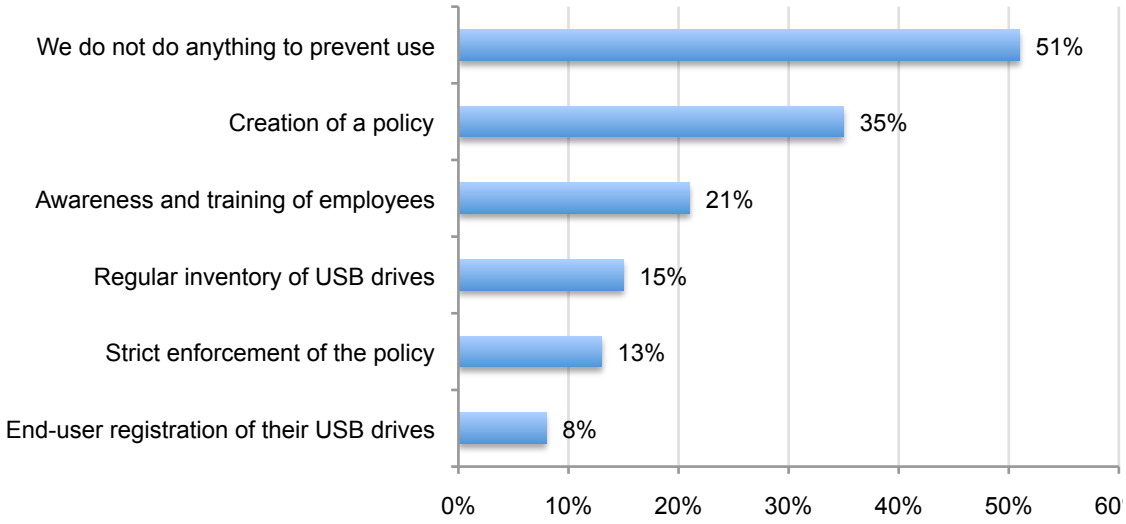
Bar Chart 7 shows how organizations attempt to vet USB reliability. According to 48 percent of respondents, organizations do not test for reliability and integrity in advance of use by employees. About one-third of respondents (32 percent) say their organizations test devices for malicious code. Thirty percent say they confirm USB drive compliance with leading security standards (such as FIPS-2) before purchasing them.

Bar Chart 7: How do organizations determine USB drive reliability and integrity?



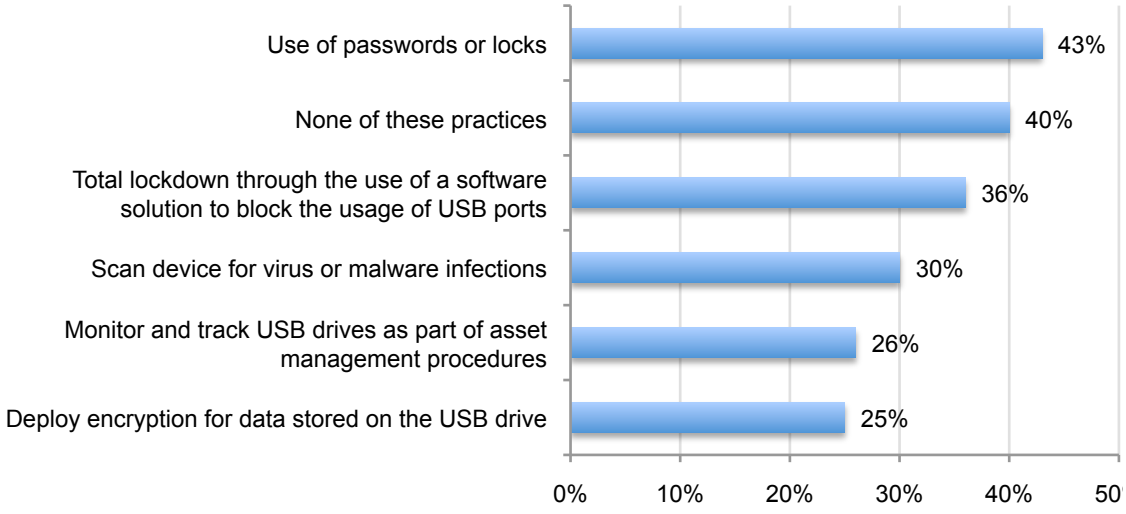
According to Bar Chart 8, to keep low quality USBs out of the hands of their employees, more than half (51 percent) of respondents say their organization does not do anything. Thirty-five percent say they have a policy and 21 percent they have awareness and training initiatives for their employees.

Bar Chart 8: How do organizations prevent low quality, off-the-shelf or free USB drives from being used in the workplace?



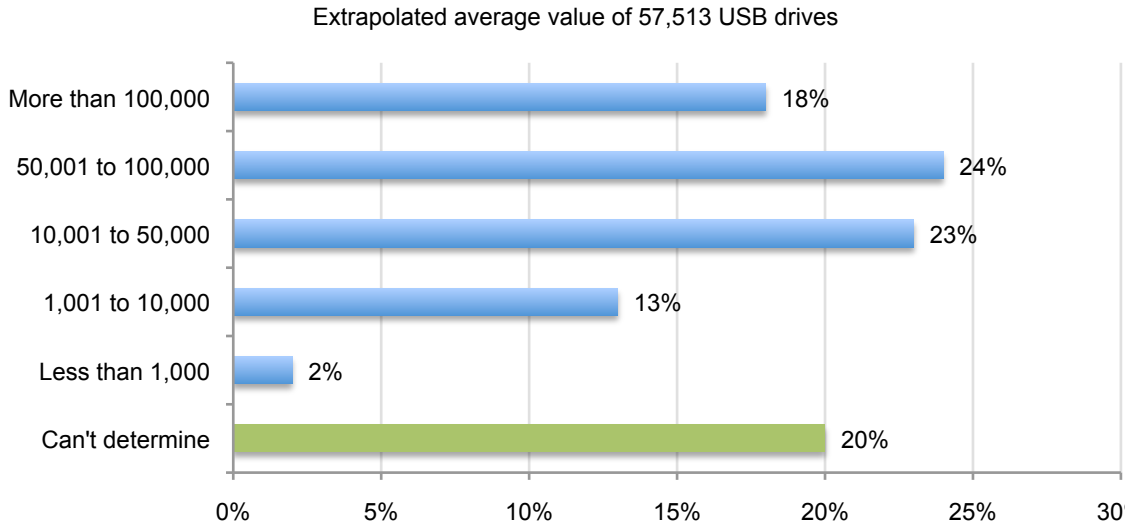
In addition, a large number of respondents say their organization is not required to adopt the following security practices to increase the security of USB drives: use passwords or locks, total lockdown through the use of a software solution to block the usage of USB ports, scan devices for virus or malware infections, monitor and track USB drives as part of asset management procedures, and deploy encryption for data stored on the USB drive.

Bar Chart 9: Do organizations require any of the following security practices to increase the security of USB drives?



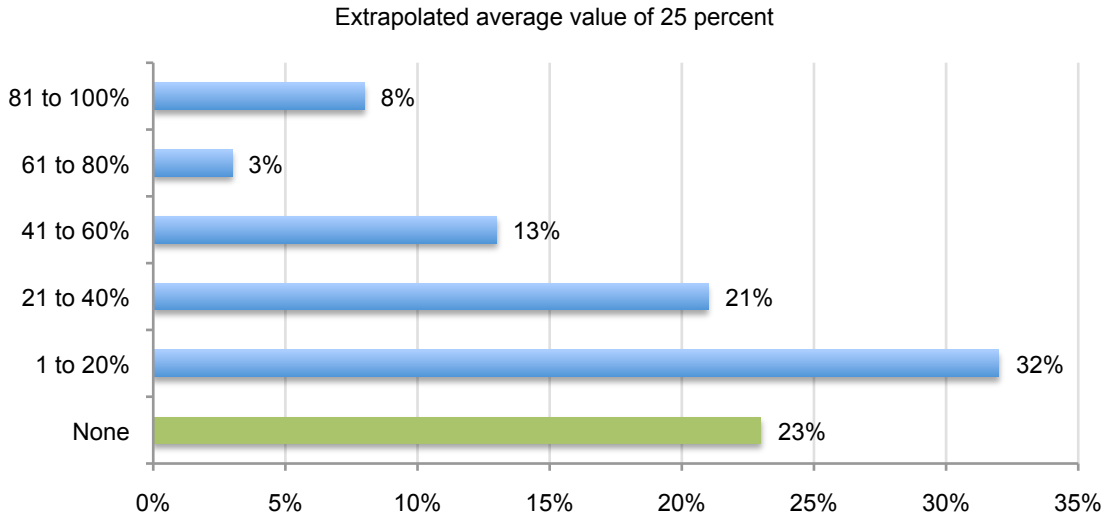
It is not surprising, based on the perceptions of respondents, that most employees' USB devices are not secure and contain confidential business information. As reported in Bar Chart 10, on average, organizations in our study report the use of more than 57,000 USB drives. Approximately 75 percent of these are not considered secure. Typically, employees download customer data, non-financial confidential documents and other intellectual properties.

Bar Chart 10. How many USB drives are used by employees within organizations today?



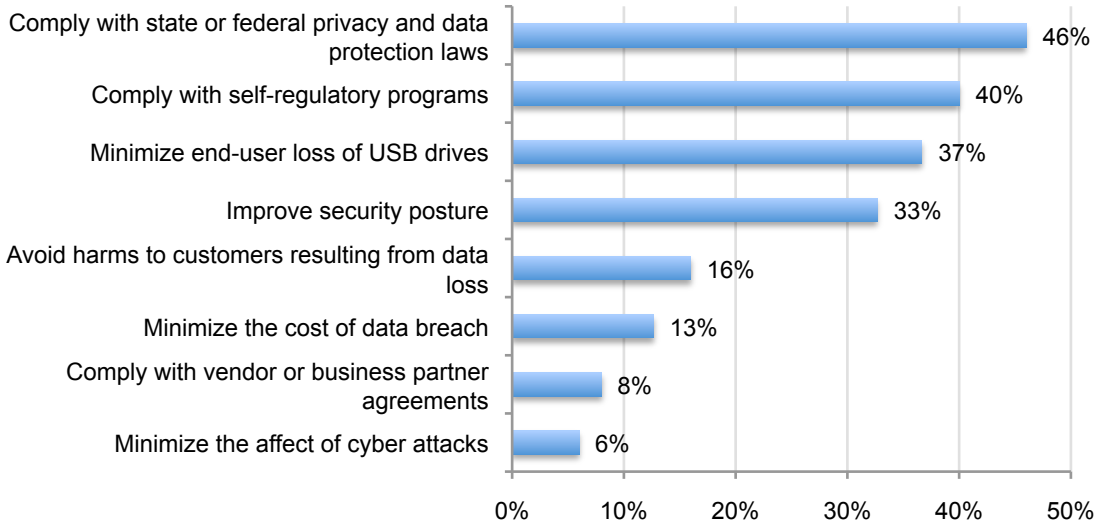
As shown in Bar Chart 11, on average 25 percent of USB drives used by employees are considered safe and secure according to respondents. The most at-risk information assets often temporarily stored on USB devices include customer data, non-financial confidential documents and other intellectual properties (including design documents and source code).

Bar Chart 11: What percent of USB drives used in the workplace are safe and secure?



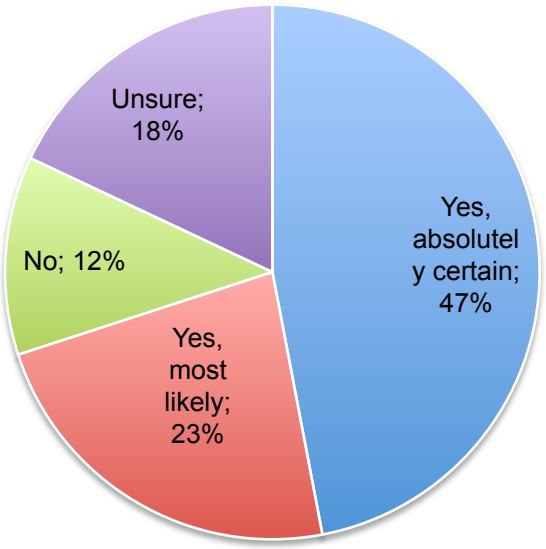
More than half (51 percent) of respondents report that they do not encrypt data stored on USB drives (not shown in the chart). If they do encrypt, it is to be in compliance with state or federal privacy and data protection laws and self-regulatory programs such as PCI DSS, ISO, NIST and others. Bar Chart 12 summarizes other reasons organizations encrypt USB drives.

Bar Chart 12: What are the main reasons why organizations encrypt data on USB drives?

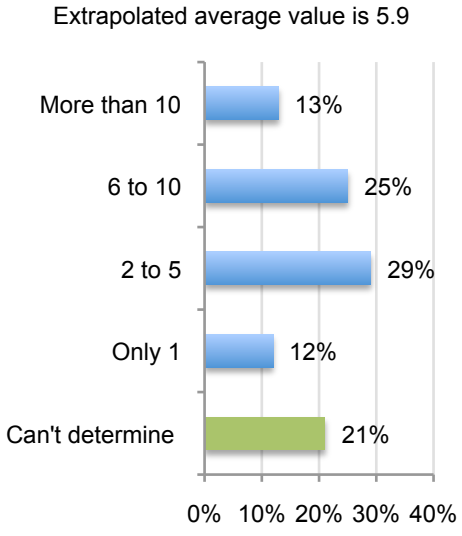


The devices may be small but the data breaches as a result of missing USBs can be devastating. Pie Chart 2 reveals that 47 percent of respondents say they are absolutely certain that their organization experienced the loss of sensitive or confidential information on a missing USB drive during the past two years. To make matters worse, respondents believe data loss or theft caused by insecure USB drives happen frequently – such as 5.9 times on average using extrapolation methods (see Bar Chart 13).

Pie Chart 2: Did your organization experience the loss of sensitive or confidential information contained on a missing USB drive sometime over the past 24 months?

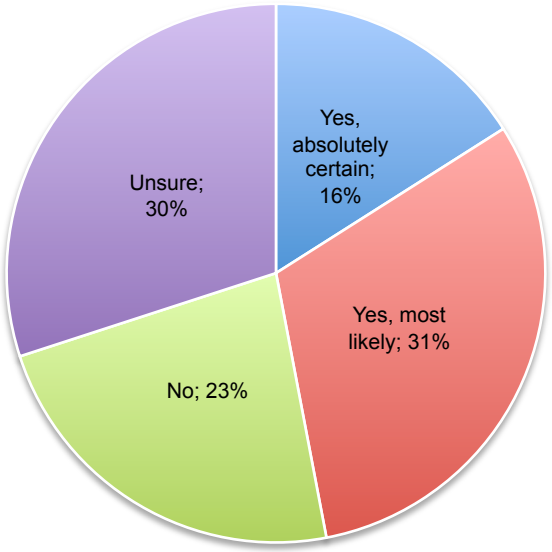


Bar Chart 13: If yes, approximately how many separate incidents involving the loss of confidential information contained on a missing USB drive occurred over the past 24 months?

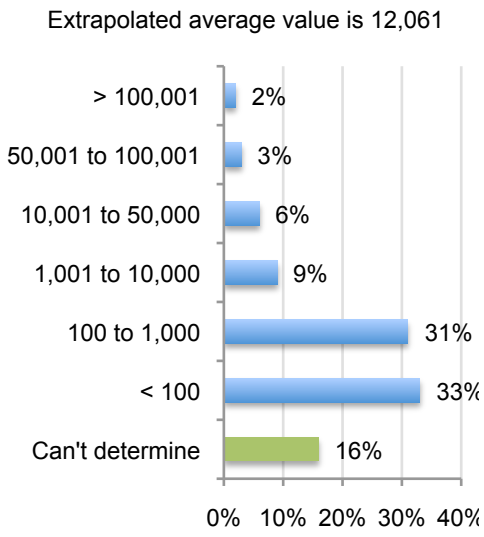


On average (see Bar Chart 14), respondents estimate that their organizations lost more than 12,000 records about customers, consumers and employees as a result of a lost or stolen USB drives over the past two years. Pie Chart 3 reveals that 40 percent of those respondents that say as a result of the lost USB drive their organization had a data breach.

Pie Chart 3: If yes, did any of these missing USB drives result in the loss or theft of data about people or households such as customer or employee data?

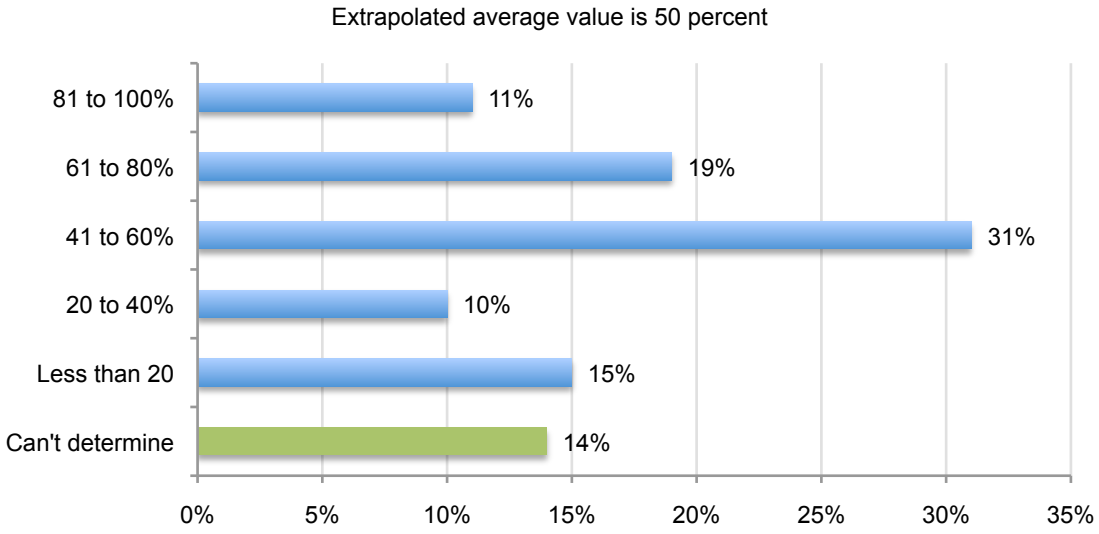


Bar Chart 14: If yes, approximately how many records were lost or stolen or as a result of missing USB drives over the past 24 months?



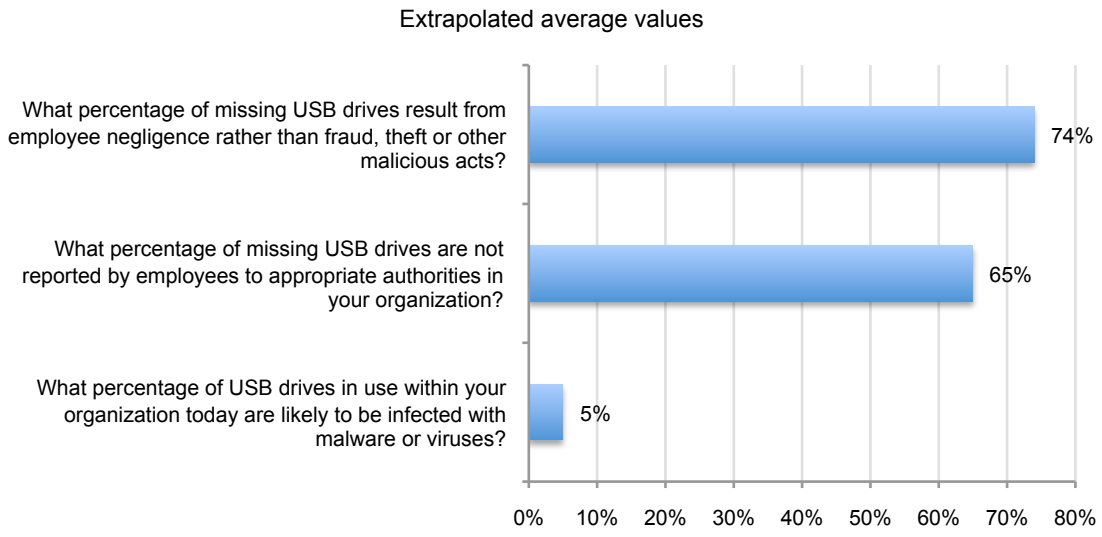
Respondents believe, on average, about half of all data lost or stolen from USB devices would be protected if the USB drive was properly encrypted.

Bar Chart 15: Approximately what percentage of lost or stolen records would have been protected from abuse if the USB drive was encrypted?



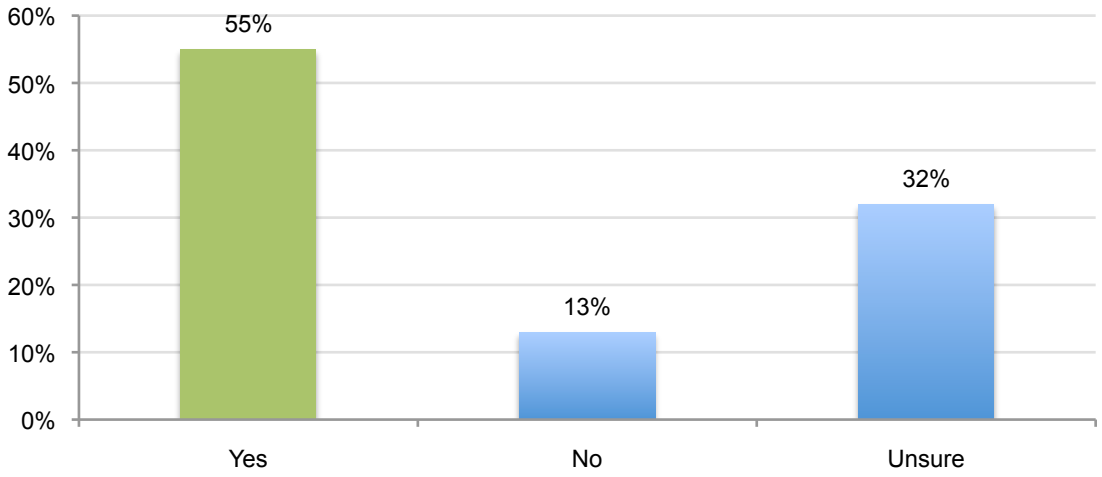
End-user negligence as opposed to maliciousness is most often the cause of missing USB drives. On average, 74 percent of missing USB drives for organizations in our study is caused by negligence. Based on this finding, training and awareness programs and policies should be the first steps organizations take to improve the state of USB security. In addition, 65 percent of respondents believe employees in the organizations will not report a lost USB drive to authorities. Finally, respondents believe on average only 5 percent of USB drives are likely to be infected with malware or viruses.

Bar Chart 16: Extrapolated average percentage values for three USB drive security issues



Despite the low infection rate mentioned above, as shown in Bar Chart 17, more than 55 percent of respondents believe malware-infected USB drives cause the loss of information assets contained on insecure USB drives.

Bar Chart 17: Do malware-infected USB drives ever cause the loss or theft of confidential information contained on this device?



Part 3. Methods

Table 1 summarizes the sample response for this study conducted over a five-day period ending in June 2011. Our sampling frame of practitioners consisted of 20,779 individuals located in the United States who have bona fide credentials in the IT or IT security fields. From this sampling frame, we invited 19,511 individuals. This resulted in 856 individuals completing the survey of which 113 were rejected for reliability issues. Our final sample was 743, thus resulting in a 3.6% response rate.

Table 1: Survey response	Freq	Pct%
Total sampling frame	20,779	100.0%
Total returns	856	4.1%
Rejected surveys	113	0.5%
Final sample	743	3.6%

On average, respondents held 9.86 years of experience in either the IT or IT security fields. Twenty-nine percent of respondents are female and 71 percent male. Table 2 shows the organizational level of respondents. As shown, 51 percent of respondents are above the supervisory level.

Table 2: Respondents' organizational level	Pct%
Senior Executive	2%
Vice President	1%
Director	15%
Manager	33%
Supervisor	15%
Technician	24%
Staff	5%
Contractor	3%
Other	2%
Total	100%

Table 3 shows the headcount (size) of respondents' business companies or government entities. As can be seen, 52 percent of respondents are employed by larger-sized organizations with more than 5,000 individuals.

Table 3: Worldwide headcount of respondents' organizations	Pct%
Less than 500 people	11%
500 to 1,000 people	13%
1,001 to 5,000 people	24%
5,001 to 25,000 people	29%
25,001 to 75,000 people	15%
More than 75,000 people	8%
Total	100%

Pie Chart 1 shows the industry distribution for respondents who are employed by private and public sector organizations. As can be seen, the largest sectors include financial services (including banking, insurance, credit cards, investment management), public sector (including federal, state and local government organizations), and healthcare & pharmaceuticals.

Pie Chart 1: Industry segments of respondents' organizations

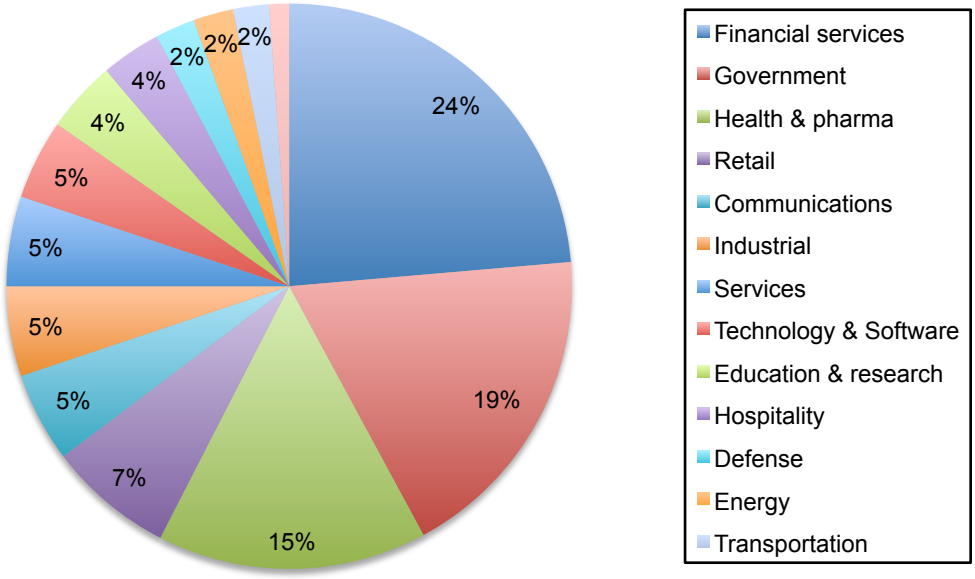


Table 4 reports the geographic footprint of respondents' organizations. In total, 74 percent of organizations have operations (headcount) in two or more countries. In addition, 60 percent have operations in one or more European nations. Finally, a total of 45 percent have operations in all major regions of the world.

Table 4: Geographic footprint of respondents' organizations	Pct%
United States	100%
Canada	63%
Europe	60%
Middle east & Africa	14%
Asia-Pacific	49%
Latin America (including Mexico)	44%

Part 4. 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 many or most organizations participating in this study do not practice. Reasons for not doing so include uncertainty about how to go about monitoring and tracking their use in the workplace, a desire not to diminish employees' productivity and a hope and belief that employees will do the right thing and immediately report if they have lost a USB drive with sensitive information.

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 70 percent of respondents in this study say they are absolutely certain or believe that 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, organizations in our study have lost more than 12,000 records about customers, consumers and employees contained on USB drives. Based on Ponemon Institute's 2010 Annual Cost of a Data Breach, the financial consequences of losing 12,000 records can cost an organization as much as $2.6 million.[1] We 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.

Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of IT and IT security practitioners, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the survey.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners who deal with data protection or information security issues. We also acknowledge that responses from paper, interviews or telephone might result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from respondents. While certain checks and balances were incorporated into our survey evaluation process, there is always the possibility that certain respondents did not provide responses that reflect their true opinions.

[1]This calculation is based on research showing the average cost of one compromised record is $214. See. 2010 Cost of Data Breach. Ponemon Institute, January 2011.

Appendix: Detailed Survey Findings

The following tables provide the percentage frequencies of responses to our survey instrument were collected and audited in June 2011. All respondents were located in the United States.

Part 1: Attributions			
Please rate the following six statements using the scale provided below each item.	Strongly agree	Agree	Combined
Q1a. My organization views the protection of confidential and sensitive information collected and temporarily stored on USB drives as a high priority.	11%	18%	29%
Q1b. My organization is willing to pay a premium to ensure USB drives used by employees are safe and secure.	12%	13%	25%
Q1c. My organization has adequate governance procedures, controls and policies to stop or curtail employee misuse of USB drives in the workplace.	10%	19%	29%
Q1d. My organization has appropriate technologies to prevent or quickly detect the downloading of confidential data onto USB drives by unauthorized parties.	10%	16%	26%
Q1e. My organization has appropriate technologies to prevent or quickly detect virus or malware infections that may reside on USB drives before use by employees in the workplace.	10%	16%	26%
Q1f. The use of encryption to secure USB drives makes sense for my organization.	26%	31%	57%
Q1g. The use of USB drives increases the productivity of employees in the workplace.	25%	28%	53%
Q1h. Employees' use of USB drives improves the efficiency of IT operations in my organization.	21%	25%	46%

Part 2. Practices			
Q2. How frequently do the following situations occur within your organization? All the time, very frequently (combined response)	All the time	Very frequent	Combined
Q2a. Employees (end-users) use USB drives without obtaining advance permission to do so.	50%	28%	78%
Q2b. Employees (end-users) lose USB drives without notifying appropriate authorities about this incident.	49%	24%	73%
Q2c. Employees (end-users) use generic USB drives such as those received "free" at conferences, trade events or business meetings.	52%	20%	72%

Q3a. Does your organization provide employees with approved USB drives for use in the workplace?	Pct%
Yes	38%
No	50%
Unsure	12%
Total	100%

Q3b. If yes, despite availability of approved USB drives, what percentage of employees use generic or unapproved USB drives in the workplace?	Pct%
None	0%
1 to 20%	14%
21 to 40%	15%
41 to 60%	20%
61 to 80%	21%
81 to 100%	30%
Total	100%

Q4a. Does your organization have a policy that describes the acceptable or unacceptable uses of USB drives for employees in the workplace?	Pct%
Yes	48%
No	40%
Unsure	12%
Total	100%

Q4b. If yes, does the acceptable use policy require that employees who have access to sensitive and confidential data only use secure USB drives?	Pct%
Yes	44%
No	39%
Unsure	17%
Total	100%

Q4c. If yes, how does your organization enforce compliance with this policy? Please select all that apply.	Pct%
Asset tracking	19%
Data loss prevention tools	21%
Network intelligence tools	13%
Random inspections	20%
Internal audits	13%
Supervisory monitoring	34%
Employee training	29%
Not enforced (Go to Q4d)	58%
Unsure	12%
Total	219%

Q4d. If not enforced, why? Select all that apply.	Pct%
We do not have the tools or resources to monitor compliance	60%
We do not want to hinder the productivity of employees	58%
The misuse of USB drives is not a big problem and doesn't warrant compliance monitoring	20%
Multilayered security methods prevent insecure or unsafe USB drives from damaging data or systems	26%
We rely on employee integrity and thus trust they will not violate the policy (honor code)	46%
Other	2%
Total	212%

Q5a. Please select the top three criteria most important for your organization when purchasing USB drives.	Pct%
Price	70%
Ease of use	14%
End-user support tools	16%
Ability to prevent such attacks as malware, botnets, viruses	54%
Compatibility with high-level encryption standards	37%
Manageability and usage controls	16%
Security certification and testing	52%
Other (please specify)	3%
Total	262%

Q5b. Please select the top three criteria most important for your organization when purchasing other memory or storage technologies.	Pct%
Price	69%
Ease of use	20%
End-user support tools	26%
Ability to prevent such attacks as malware, botnets, viruses	55%
Compatibility with high-level encryption standards	42%
Manageability and usage controls	23%
Security certification and testing	53%
Other (please specify)	2%
Total	290%

Q6. How does your organization determine USB drive reliability and integrity?	Pct%
Before purchasing, we confirm compliance with leading security standards	30%
Before using, we test to ensure there is no malicious code on these tools	32%
Before using, we test to ensure that data on the device is not corrupted	39%
We only purchase from trusted vendors	46%
We do not test for reliability and integrity	48%
Other (please specify)	2%
Total	197%

Q7. How does your organization prevent low quality, off-the-shelf or free USB drives from being used in the workplace?	Pct%
Awareness and training of employees	21%
Creation of a policy	35%
Strict enforcement of the policy	13%
End-user registration of their USB drives	8%
Regular inventory of USB drives	15%
We do not do anything to prevent low quality devices from being used	51%
Other (please specify)	3%
Total	146%

Q8. Does your organization require any of the following security practices to increase the security of USB drives? Please select all that apply.	Pct%
Use of passwords or locks	43%
Monitor and track USB drives as part of asset management procedures	26%
Deploy encryption for data stored on the USB drive	25%
Scan device for virus or malware infections	30%
Total lockdown through the use of a software solution to block the usage of USB ports	36%
None of the above	40%
Other (please specify)	5%
Total	205%

Part 3. Experience	
Q9a. Approximately (best guess), how many USB drives are used by employees (end-users) in your organization today?	Pct%
Less than 100	0%
100 to 1,000	2%
1,001 to 10,000	13%
10,001 to 50,000	23%
50,001 to 100,000	24%
More than 100,000	18%
Cannot determine	20%
Total	100%
Extrapolated value	57513

Q9b. Approximately (best guess), what percent of USB drives used by employees (end-users) in your organization are safe and secure?	Pct%
None	23%
1 to 20%	32%
21 to 40%	21%
41 to 60%	13%
61 to 80%	3%
81 to 100%	8%
Total	100%

Q10. What types of sensitive or confidential information do employees (end-users) in your organization “typically” download and store on an USB drive? Please check all that apply.	Pct%
Consumer data	21%
Customer data	49%
Employee records	25%
Non-financial confidential documents	48%
Financial confidential documents	13%
Source code	6%
Trade secrets	5%
Other intellectual properties	29%
Other (please specify)	3%
Total	199%

Q11. What types of sensitive or confidential information are normally encrypted when stored on a USB drive? Please check all that apply.	Pct%	Revised
Consumer data	3%	14%
Customer data	31%	63%
Employee records	23%	92%
Non-financial confidential documents	18%	38%
Financial confidential documents	10%	77%
Source code	5%	83%
Trade secrets	5%	100%
Other intellectual properties	15%	52%
We do not encrypt data stored on USB drives (Go to Q13)	51%	
Other (please specify)	0%	
Total	161%	

Q12. What are the two main reasons why your organization encrypts data on USB drives?	Pct%
Comply with state or federal privacy and data protection laws such as HIPAA, HITECH and others	46%
Comply with self-regulatory programs such as PCI DSS, ISO, NIST and others	40%
Minimize end-user data mishaps resulting from lost USB drives	37%
Comply with vendor or business partner agreements	8%
Avoid harms to customers resulting from data loss or theft	16%
Minimize the cost of data breach	13%
Minimize the affect of cyber attacks	6%
Improve security posture	33%
Other (please specify)	0%
Total	198%

Q13. How important is the requirement that USB drives meet high data security standards? Very important and important (response combined)	Very important	Important	Combined
Response	33%	28%	61%

Q14. What departments or operating units within your organization are most responsible for evaluating, purchasing, deploying and securing USB drives? Please select only one department per column.			
Departments/Operating Units	Evaluating USB drives	Purchasing USB drives	Deploying USB drives
IT operations	5%	15%	39%
IT security	22%	6%	5%
Business units	38%	40%	41%
Procurement	24%	35%	2%
Compliance & legal	9%	3%	2%
Data center management	2%	1%	11%
Other (please specify)	0%	0%	0%
Total	100%	100%	100%

Q15. Please check the maturity stage of your company's information security and data protection program. Select the one that in your opinion best describes the present state of IT security activities.	Pct%
Pre stage – IT security has not been established as a program within our company.	2%
Early stage – IT security program is just starting to become staffed and organized.	16%
Middle stage – IT security program is in existence and is starting to launch key initiatives.	44%
Late middle stage – IT security program is starting to evaluate the effectiveness of key initiatives.	23%
Mature stage – IT security program is in maintenance mode focusing on program evaluation and refinement.	15%
Total	100%

Q16. How frequently are USB drives reported as lost or missing in your organization? All the time & very frequently (response combined)	All the time	Very frequent	Combined
Response	34%	46%	80%

Q17. What procedures are in place to recover or secure missing UBS devices? Please select all that apply.	Pct%
End-users required to contact help desk immediately	13%
Remote termination of device (kill switch)	2%
Bounty program (finder's fee)	5%
Image backup determines what was on the device	11%
No formal procedures in place to recover lost USB drives	58%
Unsure	11%
Total	100%

Part 4. Data breach	
Q18a. Did your organization experience the loss of sensitive or confidential information contained on a missing USB drive sometime over the past 24 months?	Pct%
Yes, absolutely certain	47%
Yes, most likely	23%
No (Go to Q20)	12%
Unsure (Go to Q20)	18%
Total	100%

Q18b. If yes, approximately how many separate incidents involving the loss of sensitive or confidential information contained on a missing USB drive occurred over the past 24 months?	Pct%
Only 1	12%
2 to 5	29%
6 to 10	25%
More than 10	13%
Cannot determine	21%
Total	100%
Extrapolated value	5.9

Q18c. If yes, did any of these missing USB drives result in the loss or theft of data about people or households such as customer, consumer or employee data?	Pct%
Yes, absolutely certain	16%
Yes, most likely	31%
No (Go to Q20)	23%
Unsure (Go to Q20)	30%
Total	100%

Q18d. If yes, approximately how many records were lost or stolen or as a result of missing USB drives over the past 24 months?	Pct%
Less than 100	33%
100 to 1,000	31%
1,001 to 10,000	9%
10,001 to 50,000	6%
50,001 to 100,001	3%
100,001 to 500,000	2%
500,001 to 1 million	0%
More than 1 million	0%
Cannot determine	16%
Total	100%

Q18e. If yes, approximately what percentage of these lost or stolen records would have been protected from abuse if the USB drive was encrypted?	Pct%
None	6%
1 to 20%	9%
21 to 40%	10%
41 to 60%	31%
61 to 80%	19%
81 to 100%	11%
Cannot determine	14%
Total	100%

Q19. Approximately what percentage of missing USB drives are not reported by employees to appropriate authorities in your organization?	Pct%
None	0%
1 to 20%	6%
21 to 40%	10%
41 to 60%	13%
61 to 80%	28%
81 to 100%	30%
Cannot determine	13%
Total	100%

Q20. Approximately what percentage of missing USB drives result from employee (end-user) negligence rather than fraud, theft or other malicious acts?	Pct%
None	0%
1 to 20%	3%
21 to 40%	5%
41 to 60%	13%
61 to 80%	18%
81 to 100%	50%
Cannot determine	11%
Total	100%

Q21a. Approximately what percentage of USB drives in use within your organization today are likely to be infected with malware or viruses.	Pct%
None	14%
1 to 5%	18%
6 to 10%	11%
11 to 20%	3%
More than 20%	3%
Cannot determine	51%
Total	100%

Q21b. Do malware-infected USB drives ever cause the loss or theft of confidential information contained on this device?	Pct%
Yes	55%
No	13%
Unsure	32%
Total	100%

Part 5. Your role and organization	
D1. What organizational level best describes your current position?	Pct%
Senior Executive	2%
Vice President	1%
Director	15%
Manager	33%
Supervisor	15%
Technician	24%
Staff	5%
Contractor	3%
Other	2%
Total	100%

D2. Is this a full time position?	Pct%
Yes	98%
No	2%
Total	100%

D3. Check the **Primary Person** you or your IT or IT security leader reports to within the organization.	Pct%
CEO/Executive Committee	0%
Chief Financial Officer	3%
General Counsel	2%
Chief Information Officer	60%
Compliance Officer	9%
Human Resources VP	2%
Chief Information Security Officer CISO)	15%
Chief Risk Officer	6%
Other	3%
Total	100%

Total years of relevant experience	Mean	Median
D4a. Total years of IT or security experience	9.86	10.0
D4b. Total years in current position	4.12	4.5

Gender	Pct%
Female	29%
Male	71%
Total	100%

D6. What industry best describes your organization's industry focus?	Pct%
Airlines	1%
Automotive	1%
Brokerage & Investments	2%
Communications	4%
Chemicals	1%
Credit Cards	3%
Defense	2%
Education	3%
Energy	2%
Entertainment and Media	1%
Federal Government	12%
Food Service	1%

D6. Industry continued	
Healthcare	11%
Hospitality	3%
Manufacturing	4%
Insurance	2%
Internet & ISPs	1%
State or Local Government	6%
Pharmaceuticals	4%
Professional Services	3%
Research	1%
Retailing	6%
Retail Banking	16%
Services	2%
Technology & Software	4%
Transportation	0%
Total	100%

D7. Where are your employees located? (Check all that apply):	Pct%
United States	100%
Canada	63%
Europe	60%
Middle east & Africa	14%
Asia-Pacific	49%
Latin America (including Mexico)	44%

D8. What is the worldwide headcount of your organization?	Pct%
Less than 500 people	11%
500 to 1,000 people	13%
1,001 to 5,000 people	24%
5,001 to 25,000 people	29%
25,001 to 75,000 people	15%
More than 75,000 people	8%
Total	100%

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**,we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.