Ponemon INSTITUTE

The State of USB Drive Security in Europe

Sponsored by Kingston Technology

Independently conducted by Ponemon Institute LLC

Publication Date: November 2011

The State of USB Drive Security in Europe

Ponemon Institute, November 2011

Part 1. Introduction

Sponsored by Kingston Technology, Ponemon Institute is pleased to present the results of *The State of USB Drive Security in Europe*. 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. Approximately two-thirds (67 percent) of respondents say their organizations do not have appropriate technologies to prevent or quickly detect virus or malware infections that may reside on USB drives before used by employees in the workplace and 71 percent say they do not have the technologies to prevent or quickly detect the download of confidential data onto USB drives by unauthorized individuals.

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 62 percent of respondents in this study say that they are absolutely certain (31 percent) or believe that it was most likely (31 percent) 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 our 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.

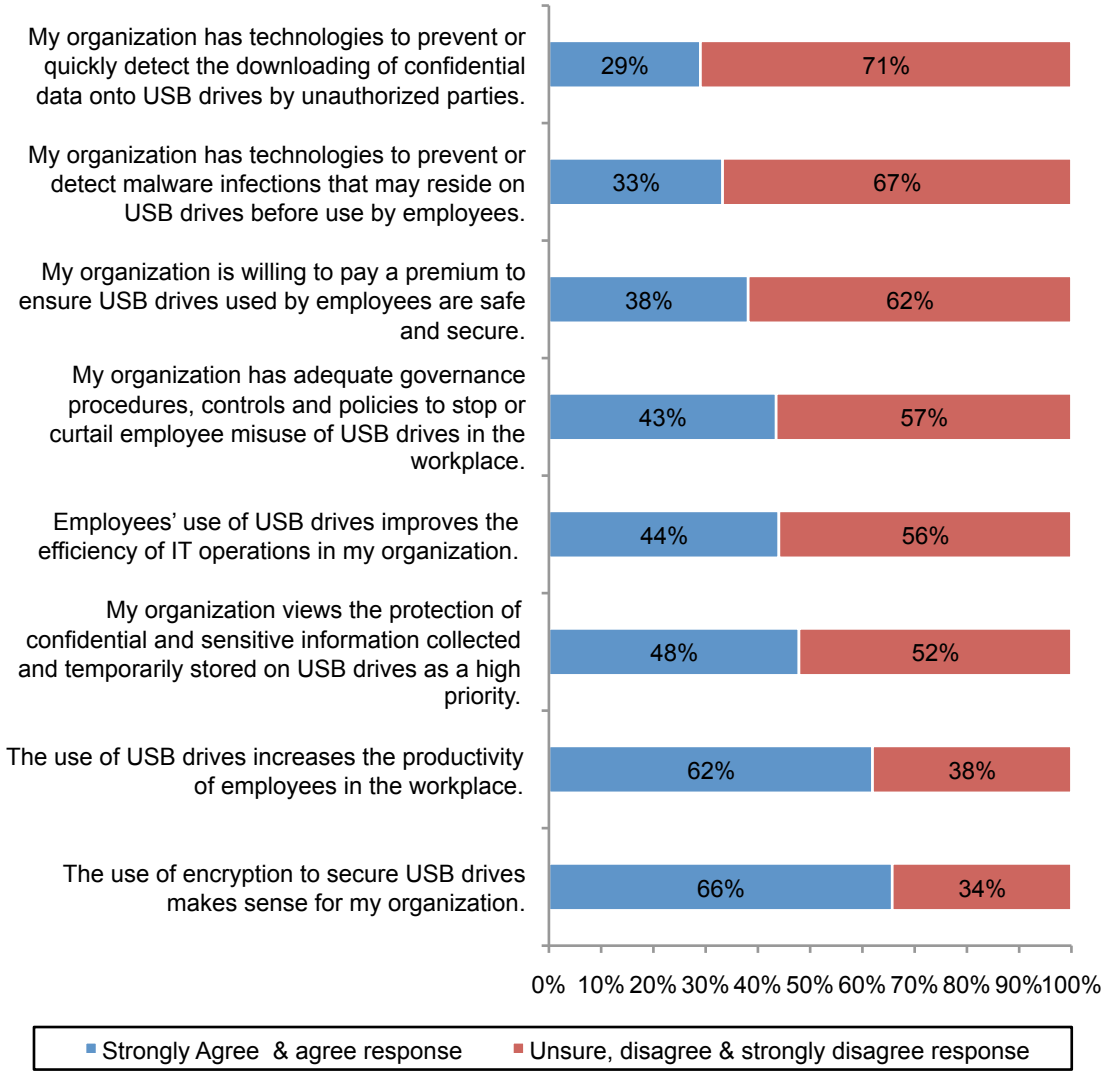
We surveyed 2,942 IT practitioners with an average of 10.75 years of IT or IT security experience In the United Kingdom, France, Germany, Denmark, Norway, Sweden, Finland, Netherlands, Switzerland and Poland. In this report, we present the consolidated findings from all countries. Most of the respondents report to the chief information officer or chief information security officer (59 percent and 11 percent, respectively). The vast majority of these respondents (77 percent) 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.

Part 2. Key Findings

Organizations are ignoring the risk of unencrypted USB drives. As shown in Bar Chart 1, more than half (52 percent) of respondents do not agree that their organizations consider the protection of confidential and sensitive information collected and temporarily stored on USB drives a high priority. This is evidenced by the belief of 71 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. Sixty-seven percent say their organizations do not have technologies to prevent or quickly detect virus or malware infections that may reside on USB drives.

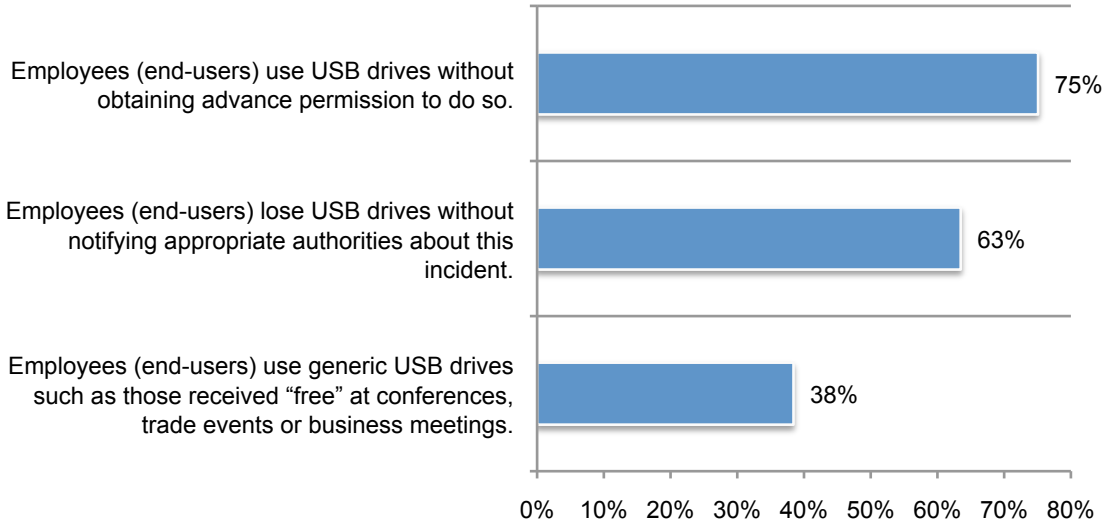
Bar Chart 1: Respondents' perceptions about USB drive security in their organizations
Five-point scale from strongly agree to strongly disagree[1]



[1]We use this five-point scale to capture respondents' perceptions or beliefs about key issues within their organization. A strongly agree and agree response at or above 50 percent is viewed as a net favorable response. In contrast, a strongly disagree, disagree and unsure response at or above 50 percent is viewed as net unfavorable.

Employees are negligent when using USB drives and this is putting organizations' sensitive data at risk. Bar Chart 2 reveals what employees are doing all the time or frequently: using USB drives without obtaining advance permission to do so (75 percent); losing USB drives without notifying appropriate authorities about this incident (63 percent) and using generic USB drives such as those received free at conferences, trade events and business meetings (38 percent).

Bar Chart 2. How frequently do the following situations occur within your organization?
All the time & very frequently combined response



Despite awareness of employees' misuse, the majority of respondents (62 percent) say their organizations are not willing to pay a premium to ensure USB drives are safe and secure. However, as shown in Pie Chart 1, 52 percent say their organizations do provide approved USB drives but most employees continue to use generic and potentially unsafe USB drives in the workplace (see Table 1).

Pie Chart 1. Does your organization provide employees with approved USB drives for use in the workplace?

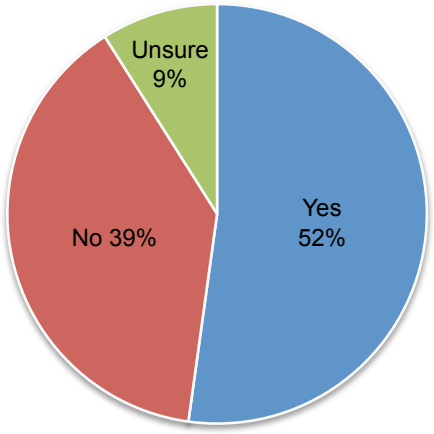
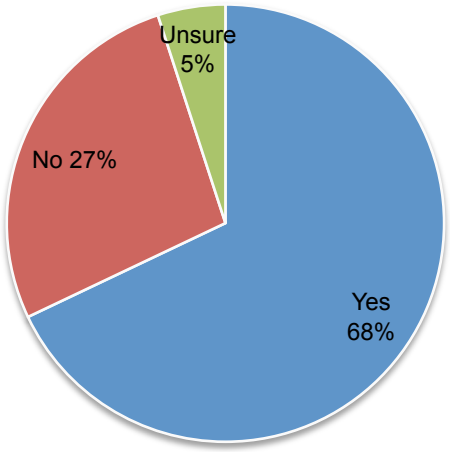


Table 1. What percentage of employees use generic or unapproved USB drives in the workplace?

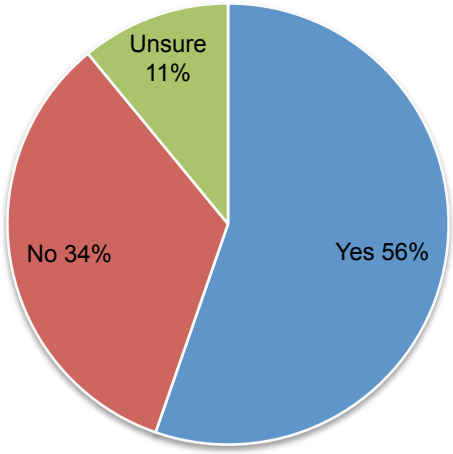
Percentage response	Pct%
None	4%
1 to 20%	12%
21 to 40%	14%
41 to 60%	23%
61 to 80%	23%
81 to 100%	24%
Total	100%

More organizations could improve the state of USB security by enforcing policies that define the acceptable use of USB drives. As shown in Pie Chart 2, 68 percent of respondents say their organizations have a policy concerning the use of USB drives. However, Pie Chart 3 reveals that 34 percent of respondents say the policy does not require employees to only use secure USB drives if they have access to sensitive and confidential data. Another 11 percent are unsure.

Pie Chart 2. Does your organization have a policy that describes the acceptable use of USB drives for employees?



Pie Chart 3. Does the policy require employees to only use secure USB drives if they have access to sensitive and confidential data?

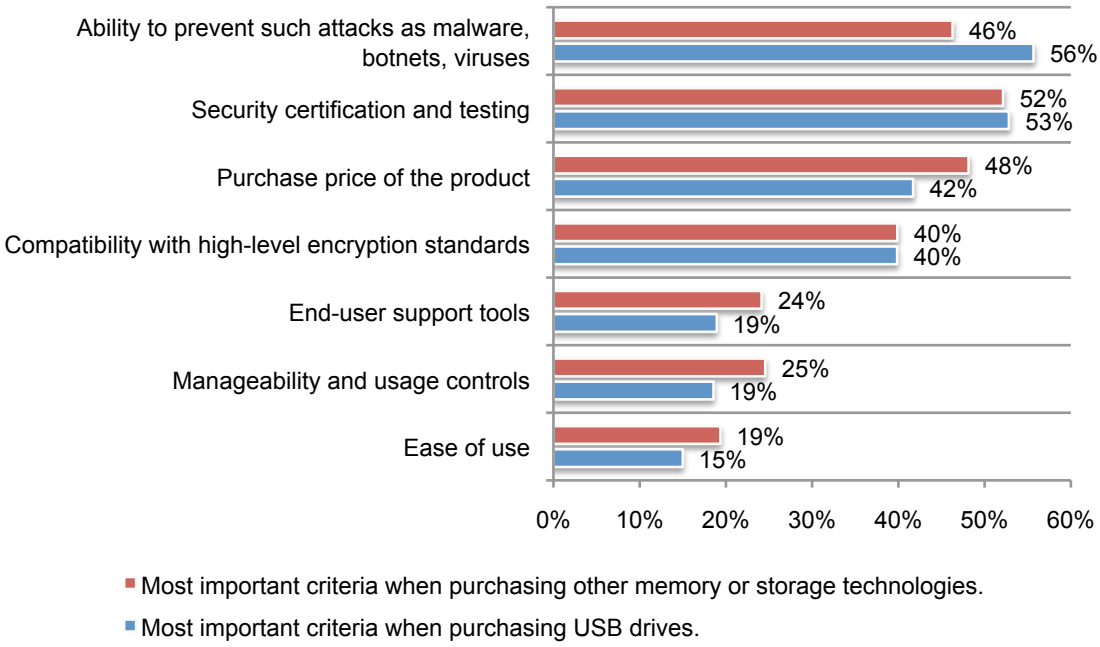


In many cases, USB security policies are meaningless because 37 percent of respondents say their organizations do not enforce compliance and 13 percent are unsure. As shown in Bar Chart 3, the primary reason for not enforcing these policies is that organizations are relying upon employee integrity and trusting they will not violate the policy.

Bar Chart 3: Why policies are not enforced
More than one response permitted

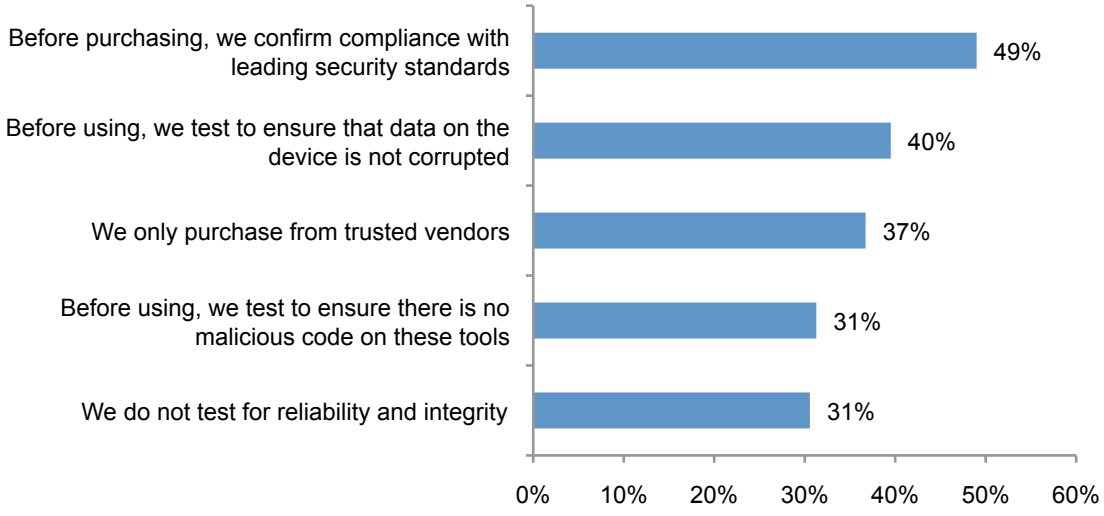
Security is more important than price when purchasing USB drives. Bar Chart 4 reveals that the ability to prevent such attacks as malware, botnets and viruses followed by security certification and testing are the top two criteria most important when purchasing USB drives. Third is price. End-user support tools and ease of use are not as important for USB drives as for other memory or storage technologies.

Bar Chart 4: The most important criteria when purchasing USB drives versus other memory or storage technologies
More than one response permitted



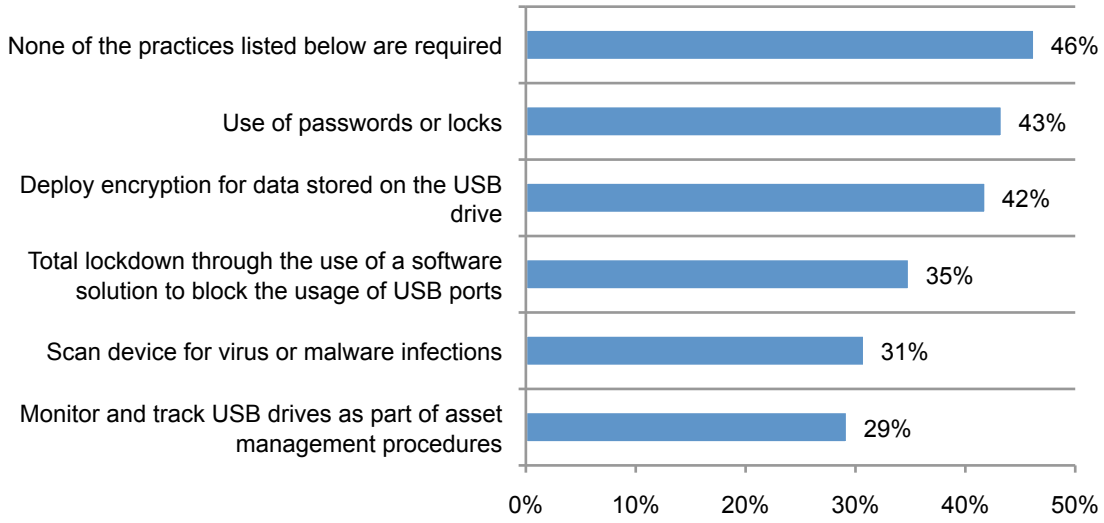
As shown in Bar Chart 5, to determine USB drive reliability and integrity, 49 percent confirm compliance with leading security standards (such as FIPs 140-2) and 40 percent test to ensure that data on the device is not corrupted. Only 31 percent test to ensure there is no malicious code on the USB drive or test for reliability and integrity.

Bar Chart 5. How does your organization determine USB drive reliability and integrity?
More than one response permitted



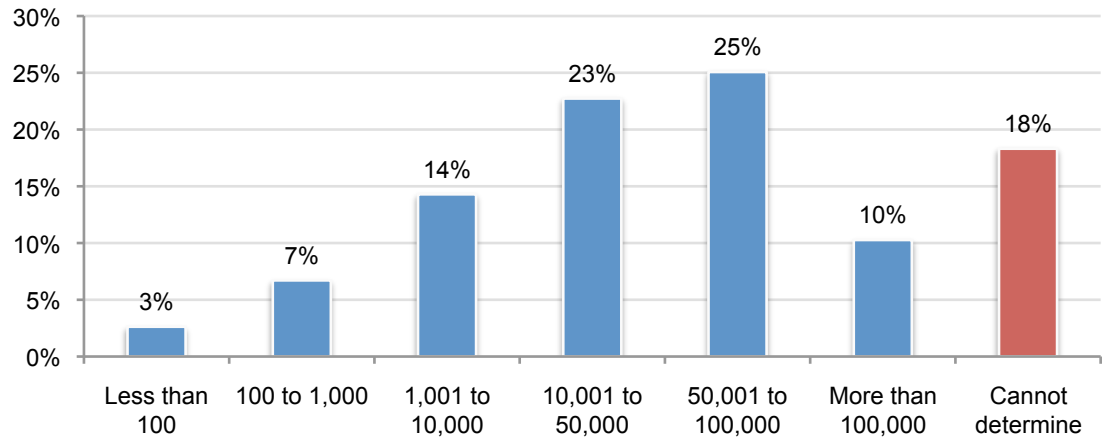
To keep low quality USBs out of the hands of their employees, 47 percent of respondents say their organization has a policy and 39 percent rely upon employee training and awareness. However, almost half (46 percent) of respondents say their organization does not require the security practices listed in Bar Chart 6 to be followed.

Bar Chart 6. Does your organization require any of the following security practices to increase the security of USB drives?
More than one response permitted



Most USB devices in the workplace are not secure and contain confidential business information. USB drives are prevalent and popular with employees. Bar Chart 7 shows that on average, organizations in our study report the use of more than 43,457 USB drives in the workplace. On average, 46 percent of these drives are not considered secure. Typically, employees download and store sensitive information about customers, confidential non-financial documents and other intellectual properties.

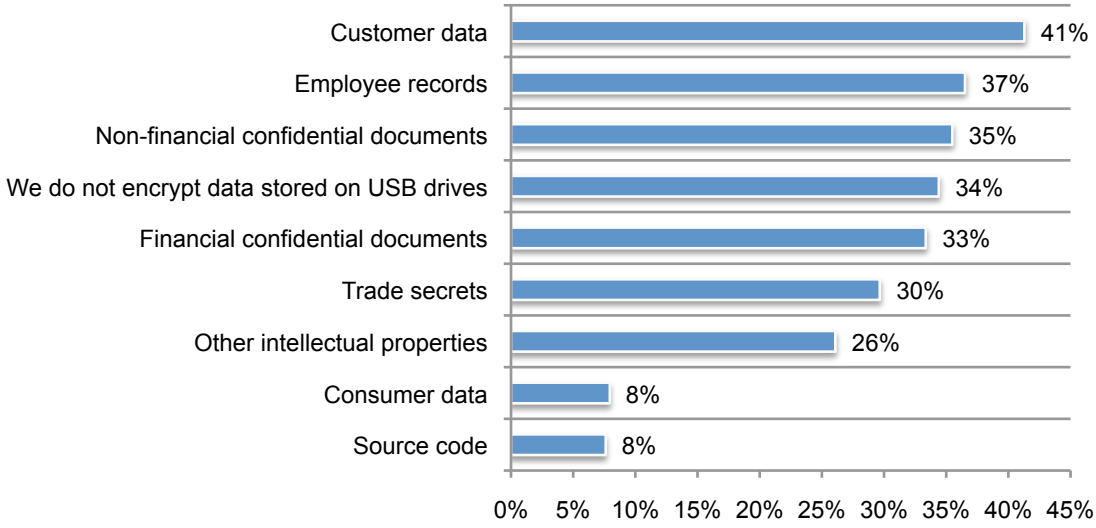
Bar Chart 7. How many USB drives are used by employees (end-users) in your organization today?
Extrapolated average value is 43,457 USB drives



According to Bar Chart 8, approximately one-third (34 percent) report that they do not encrypt data stored on USB drives. Customer data and employee records are the two types of data most often encrypted. If they do encrypt, 49 percent of respondents say it is to be in compliance with

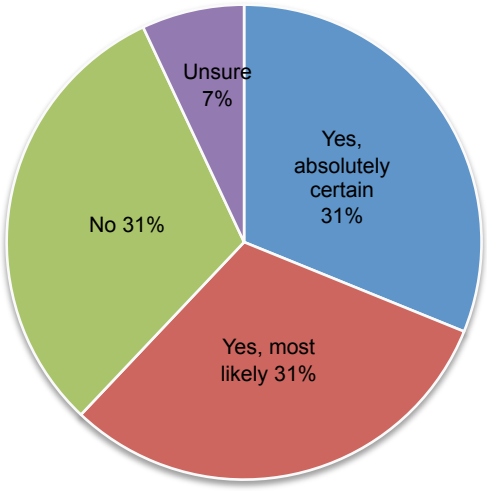
regulations/EU and nation-specific privacy laws and 38 percent say it is to comply with self-regulatory programs.

Bar Chart 8. What types of sensitive or confidential information are normally encrypted when stored on a USB drive?
More than one response permitted

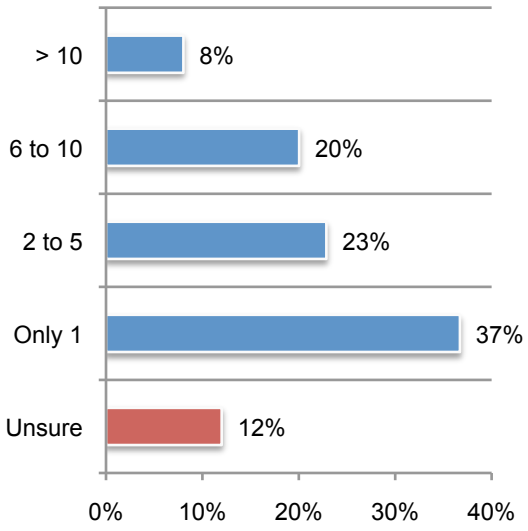


The devices may be small but the data breaches as a result of missing USBs can be devastating. Pie Chart 4 shows that more than 62 percent of respondents in this study say that they are absolutely certain (31 percent) or believe that it was most likely (31 percent) that a data breach was caused by sensitive or confidential information contained on a missing USB drive. Of those organizations reporting a data breach caused by a missing USB drive, on average there were 4.2 separate incidents involving the loss of sensitive or confidential information over the past 24 months (computed from the median range distribution shown in Bar Chart 9).

Pie Chart 4. Did your organization experience the loss of confidential information contained on a missing USB drive over the past 24 months?

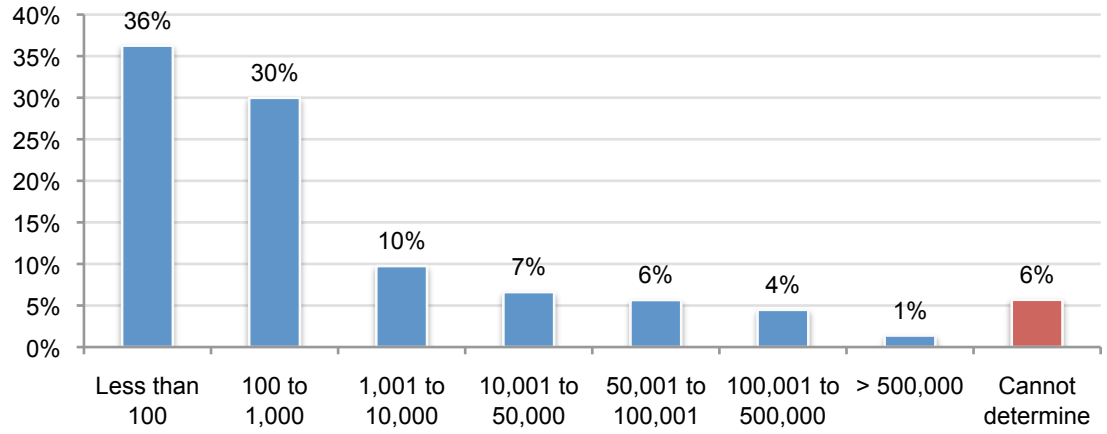


Bar Chart 9. How many separate incidents involving the loss of information contained on a missing USB drive over the past 24 months?



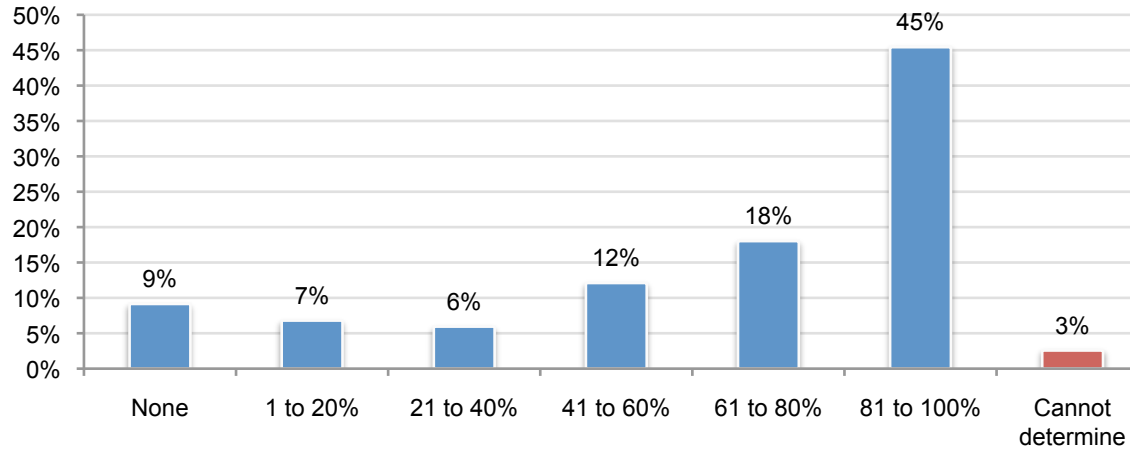
As shown in Bar Chart 10, on average organizations in our study have lost more than 34,188 records about customers, consumers and employees as a result of missing USBs. Respondents believe that on average 66 percent of these lost or stolen records could have been protected from abuse if the USB drive was encrypted.

Bar Chart 10. How many records were lost or stolen or as a result of missing USB drives over the past 24 months?
Extrapolated average value is 34,188 records



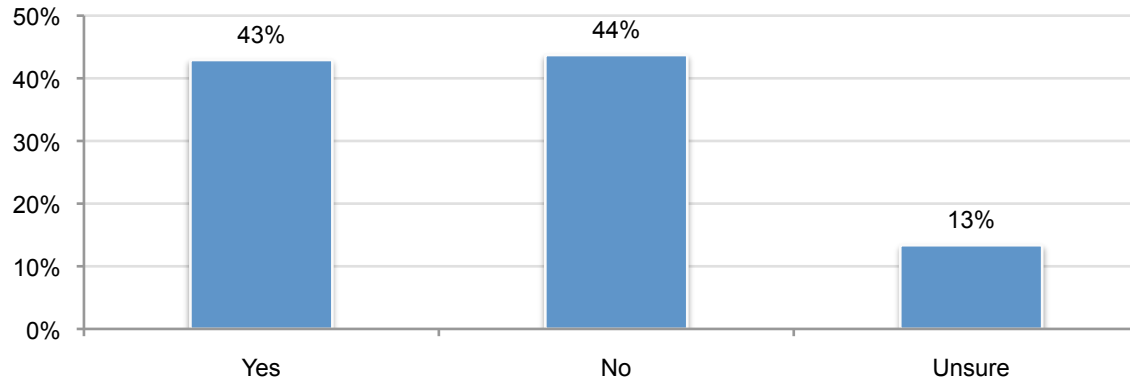
End-user negligence as opposed to maliciousness is most often the cause of missing USB drives. On average, employee negligence results in 64 percent USB drives being lost or stolen, as shown in Bar Chart 11. Based on this finding, training and awareness programs and policies should be the first steps organizations take to improve the state of USB security.

Bar Chart 11. What percentage of missing USB drives result from employee (end-user) negligence rather than fraud, theft or other malicious acts?
Extrapolated average percentage is 64 percent



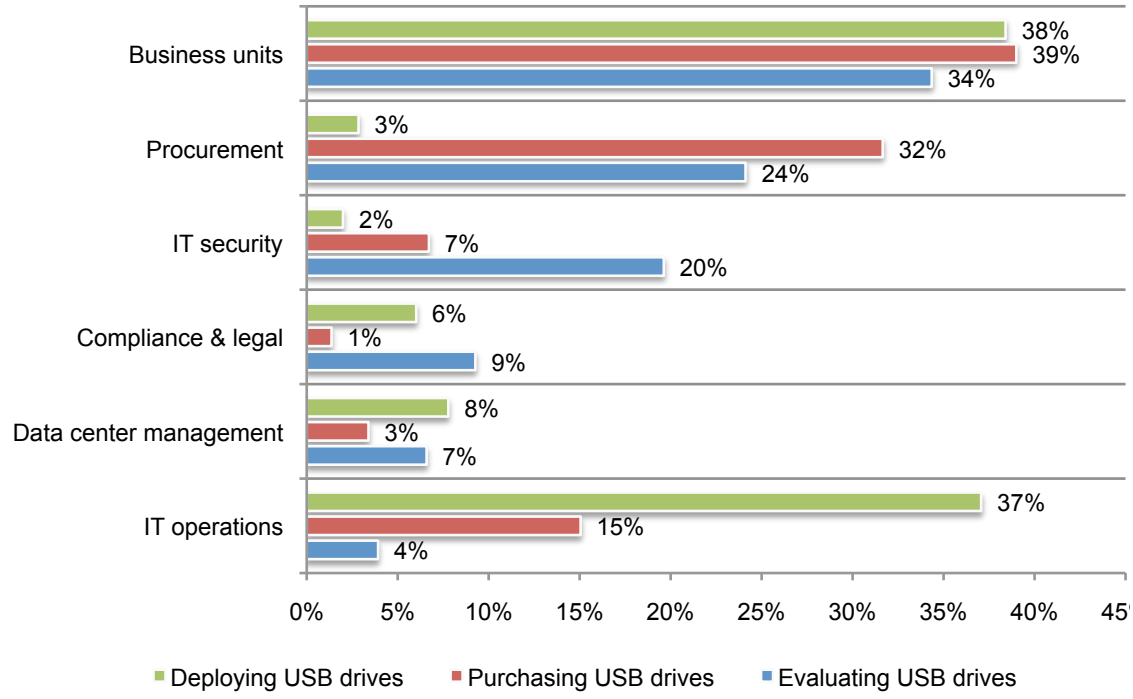
While most respondents believe it is not common for USB drives to be infected with malware or viruses, they still can create problems for an organization's sensitive and confidential information. Bar Chart 12 reveals that 43 percent of respondents say that malware-infected USB drives have caused the loss or theft of confidential information contained on the device and 13 percent are unsure.

Bar Chart 12. Do malware-infected USB drives ever cause the loss or theft of confidential information contained on this device?



IT and IT security practitioners understand the security risks but are often not involved in decisions related to the use of USB drives. As mentioned in the introduction, 77 percent of respondents believe it is very important or important that USB drives meet high data security standards. However, Bar Chart 13 shows that business units and procurement departments are most responsible for evaluating and purchasing USB drives. Thirty-eight percent of business units are responsible for deploying USB drives and a similar percentage (37 percent) of respondents say it is IT operations.

Bar Chart 13. What departments or operating units are <u>most</u> responsible for evaluating, purchasing and deploying USB drives?

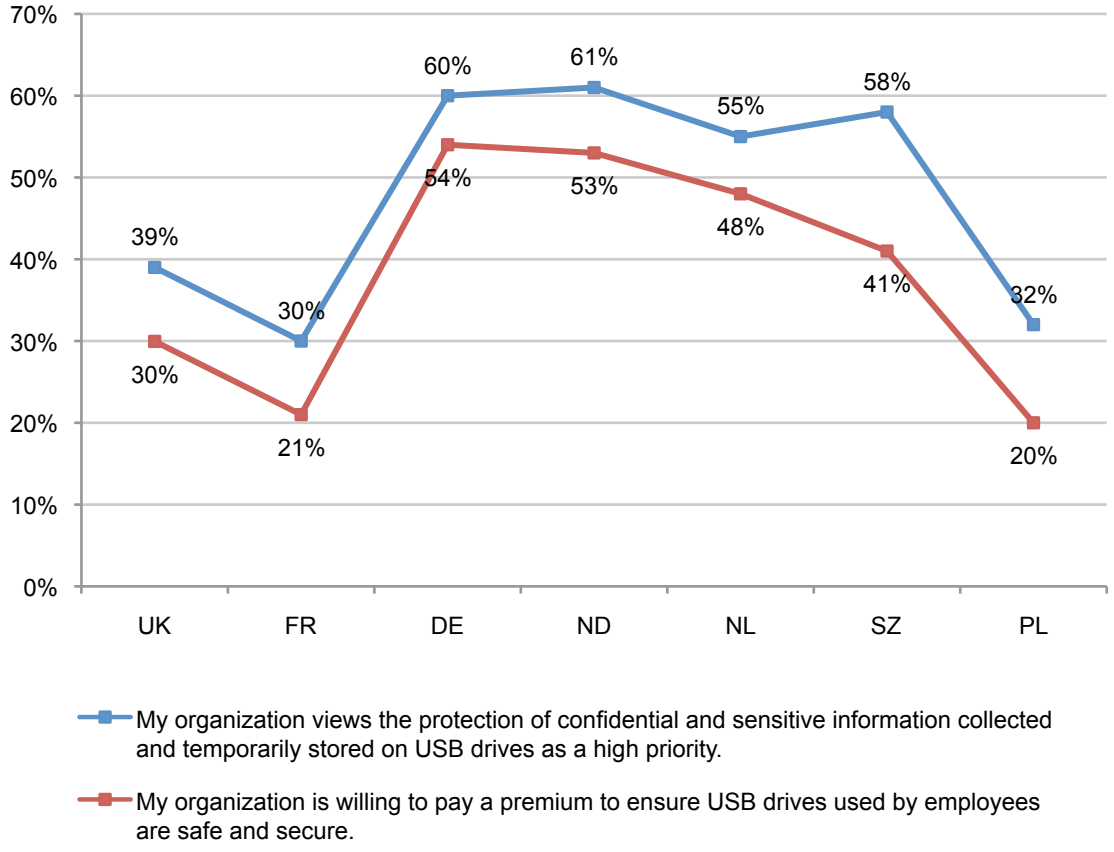


Part 3. Country Differences

The following are the most interesting country differences in perceptions and practices about USB security.

Perceptions and about the importance of USB security. As shown in **Line Graph 1,** Respondents in the Nordics[2], Germany and Switzerland are more likely to believe their organizations view the protection of confidential and sensitive information collected and temporarily stored on USB drives as a high priority. As a result, they are more likely to pay a premium to ensure USB drives used by employees are safe and secure. Organizations in the UK, Poland and France are least likely to agree this is the case. These same countries also believe their organizations would not pay a premium for a safer and more secure USB drives.

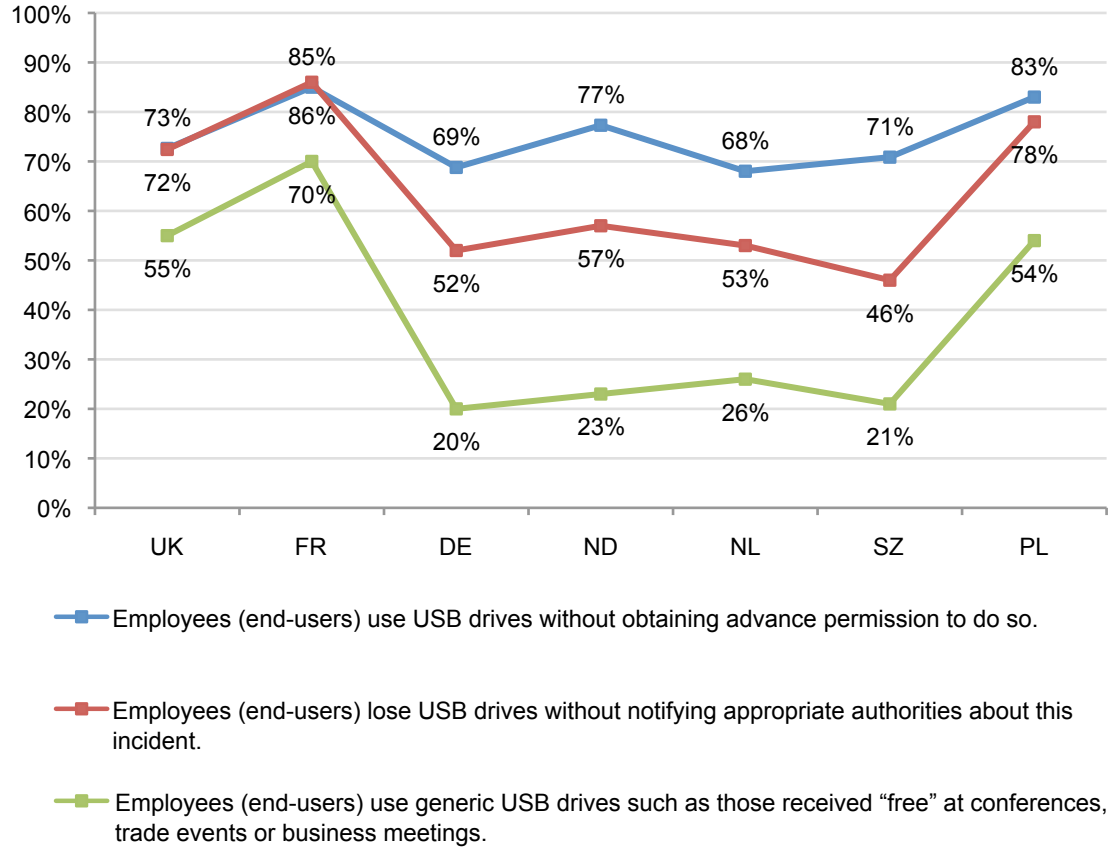
Line Graph 1. Perceptions about USB security for countries in this study
Strongly agree & agree combined response



[2] The Nordics (ND) region includes Denmark, Norway, Sweden and Finland

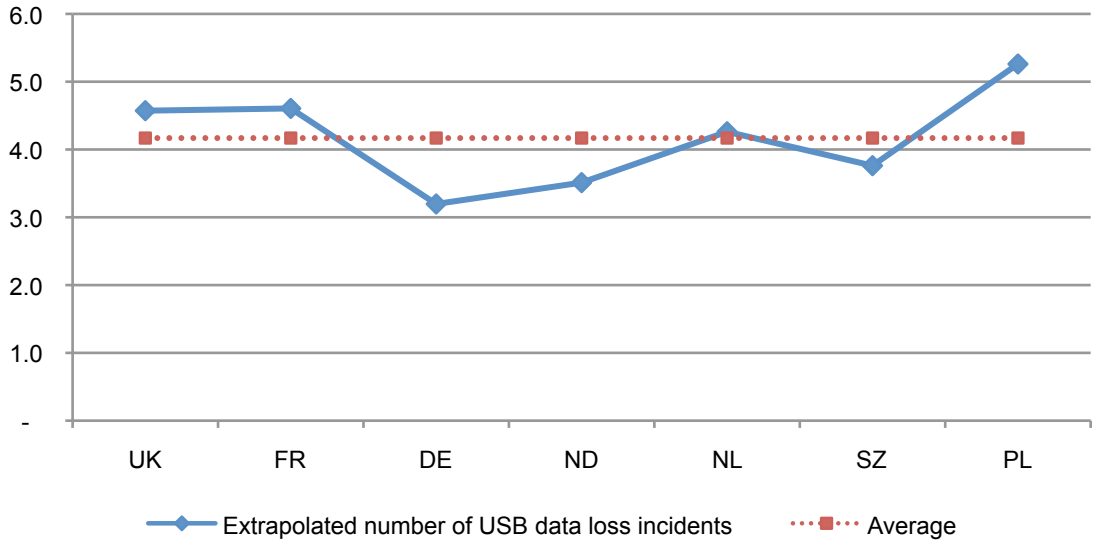
Employee practices put organizations at risk. France and Poland are most at risk as a result of employees' practices, according to Line Graph 2. Eighty-five percent of respondents in France and 83 percent of respondents in Poland say that employees use USB drives without obtaining advance permission to do so very frequently or frequently. Employees in these countries also tend not to notify authorities when they lose USB drives and use generic USB drives such as those received "free" at conferences, trade events or business meetings. Countries where employees are more careful with their USB drives are Germany, Nordics, Netherlands and Switzerland.

Line Graph 2. Three risky employee (end-user) behaviors
Happens all the time or very frequently combined response



Data breach caused as a result of a missing USB drive. Line Graph 3 reveals that countries where respondents say their organizations had the highest rate of data breach as a result of a missing USB drive are France, UK and Poland. The lowest rate was for organizations in Germany. Countries where respondents say their organizations had the greatest loss or theft of data about people or households as a result of missing USB drives are France, Poland and the Nordics.

Line Graph 3. How many separate incidents involving the loss of sensitive or confidential information contained on a missing USB drive occurred over the past 24 months?
Only those organizations that experienced a USB-related breach incident



Part 4: Methods

Table 4 reports the sample response for 7 separate country/region samples. The sample response for this study was conducted over a 30-day period ending in September 2011. Our consolidated sampling frame of practitioners in seven (7) countries (the sample responses for Denmark, Norway, Sweden and Finland were combined) consisted of 74,357 individuals who have bona fide credentials in the IT or IT security fields. From this sampling frame, we captured 3,257 returns of which 315 were rejected for reliability issues. Our final consolidated sample was 2,942, thus resulting in a 4 percent response rate.

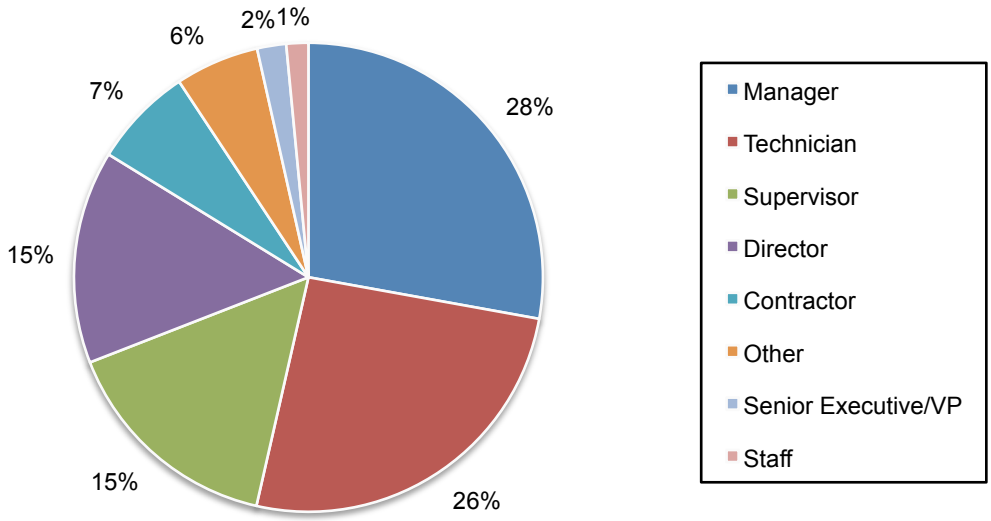
Table 2. Sample response for seven countries

Countries	Legend	Sampling frame	Total returns	Rejected surveys	Final sample	Response rate
United Kingdom	UK	12,199	504	53	451	3.7%
France	FR	13,045	513	69	444	3.4%
Germany	DE	15,698	659	47	612	3.9%
Nordics	ND	7,785	315	12	303	3.9%
Netherlands	NL	10,814	502	49	453	4.2%
Switzerland	SZ	6,726	338	32	306	4.5%
Poland	PL	8,090	426	53	373	4.6%
Total		74,357	3,257	315	2,942	4.0%

The respondents' mean and median experience in IT or IT security is 10.75 and 11.0 years, respectively. Sixty-nine percent of respondents are male and 31 percent female. The primary reporting channels most frequently cited by respondents are the chief information officer (59 percent) – followed by the chief information security officer (11 percent) and the chief risk officer (8 percent).

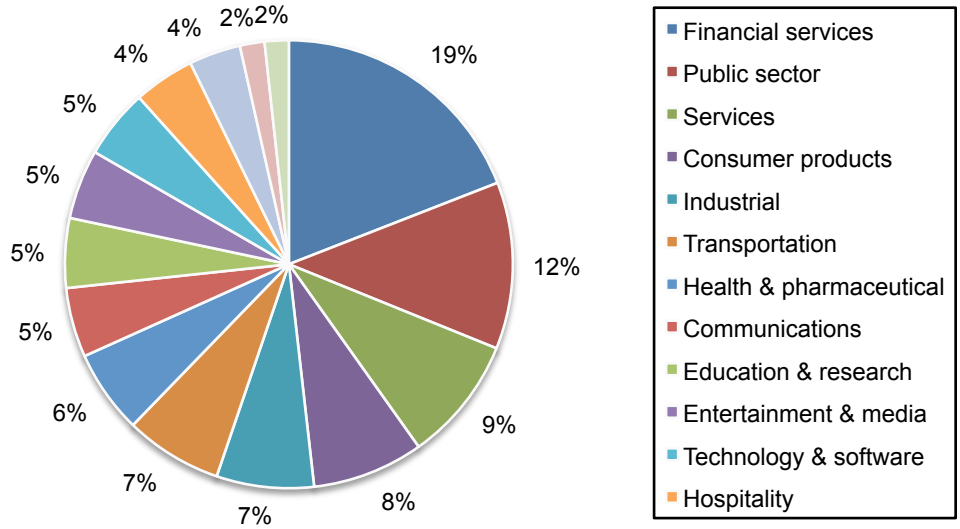
Pie Chart 5 summarizes the approximate position levels of respondents from all European countries in our study. As can be seen, the majority (60 percent) of respondents are at or above the supervisory level.

Pie Chart 5. Distribution of respondents according to position level
Consolidated for 7 separate country samples



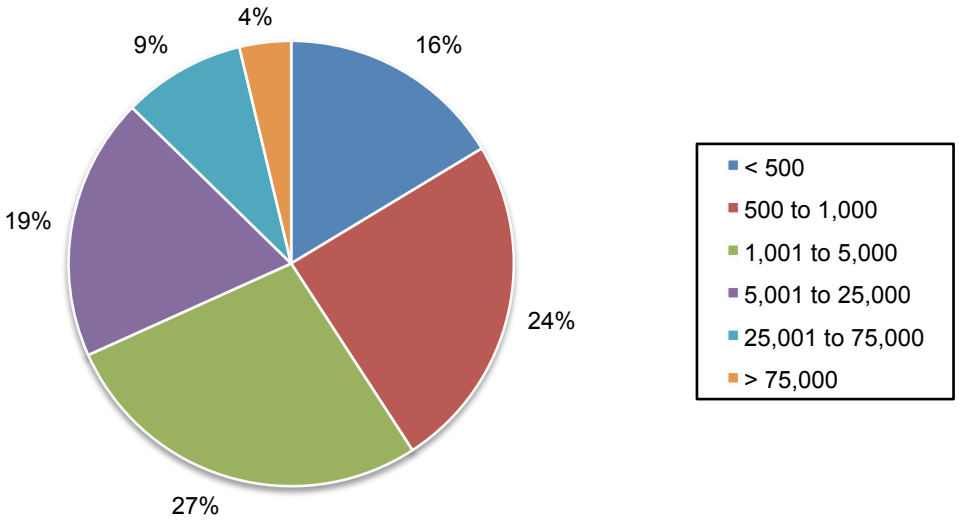
Pie Chart 6 reports the primary industry segments in this study. As shown, 19 percent of respondents are located in financial services, which includes banking, investment management, insurance, brokerage, payments and credit cards. Another 12 percent are located in public sector organizations, including central and local government.

Pie Chart 6. Distribution of respondents according to primary industry classification
Consolidated for 7 separate country samples



According to Pie Chart 7, the majority of respondents (60 percent) are located in larger-sized organizations with a global headcount of more than 1,000 employees.

Pie Chart 7: Distribution of respondents according to organizational headcount
Consolidated for 7 separate country samples



Part 5. Limitations

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 in seven countries, 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 network or 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.

Part 6. 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 more than half of respondents (52 percent) do not 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 62 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 34,188 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 France is $136, Germany it is $191 and in the United Kingdom it is $114 (these amounts were converted to U.S. dollars). 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.

Appendix: Consolidated Survey Results

The following tables report the frequencies or percentage frequencies of all survey questions completed by respondents located in seven European countries. Please note that all survey results by country were captured in August through October 2011.

Survey response	Consolidated
Total sampling frame	74,357
Total returns	3,257
Rejected surveys	315
Final sample	2,942
Response rate	4.0%

Part 1: Attributions	
Please rate the following six statements using the scale provided below each item. Strongly agree and agree (combined response)	Consolidated
Q1a. My organization views the protection of confidential and sensitive information collected and temporarily stored on USB drives as a high priority.	48%
Q1b. My organization is willing to pay a premium to ensure USB drives used by employees are safe and secure.	38%
Q1c. My organization has adequate governance procedures, controls and policies to stop or curtail employee misuse of USB drives in the workplace.	43%
Q1d. My organization has appropriate technologies to prevent or quickly detect the downloading of confidential data onto USB drives by unauthorized parties.	29%
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.	33%
Q1f. The use of encryption to secure USB drives makes sense for my organization.	66%
Q1g. The use of USB drives increases the productivity of employees in the workplace.	62%
Q1h. Employees' use of USB drives improves the efficiency of IT operations in my organization.	44%

Part 2. Practices

Q2. How frequently do the following situations occur within your organization? All the time, very frequently (combined response)	Consolidated
Q2a. Employees (end-users) use USB drives without obtaining advance permission to do so.	75%
Q2b. Employees (end-users) lose USB drives without notifying appropriate authorities about this incident.	63%
Q2c. Employees (end-users) use generic USB drives such as those received "free" at conferences, trade events or business meetings.	38%

Q3a. Does your organization provide employees with approved USB drives for use in the workplace?	Consolidated
Yes	52%
No	39%
Unsure	9%
Total	100%

Q3b. If yes, despite availability of approved USB drives, what percentage of employees use generic or unapproved USB drives in the workplace?	Consolidated
None	4%
1 to 20%	12%
21 to 40%	14%
41 to 60%	23%
61 to 80%	23%
81 to 100%	24%
Total	100%

Q4a. Does your organization have a policy that describes the acceptable or unacceptable uses of USB drives for employees in the workplace?	Consolidated
Yes	68%
No	27%
Unsure	5%
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?	Consolidated
Yes	56%
No	34%
Unsure	11%
Total	100%

Q4c. If yes, how does your organization enforce compliance with this policy? Please select all that apply.	Consolidated
Asset tracking	19%
Data loss prevention tools	36%
Network intelligence tools	37%
Random inspections	42%
Internal audits	13%
Supervisory monitoring	32%
Employee training	30%
Not enforced (Go to Q4d)	37%
Unsure	13%
Total	259%

Q4d. If not enforced, why? Select all that apply.	Consolidated
We do not have the tools or resources to monitor compliance	41%
We do not want to hinder the productivity of employees	42%
The misuse of USB drives is not a big problem and doesn't warrant compliance monitoring	18%
Multilayered security methods prevent insecure or unsafe USB drives from damaging data or systems	34%
We rely on employee integrity and thus trust they will not violate the policy (honor code)	70%
Other	5%
Total	210%

Q5a. Please select the top three criteria most important for your organization when purchasing USB drives.	Consolidated
Price	42%
Ease of use	15%
End-user support tools	19%
Ability to prevent such attacks as malware, botnets, viruses	56%
Compatibility with high-level encryption standards	40%
Manageability and usage controls	19%
Security certification and testing	53%
Other (please specify)	1%
Total	244%

Q5b. Please select the top three criteria most important for your organization when purchasing other memory or storage technologies.	Consolidated
Price	48%
Ease of use	19%
End-user support tools	24%
Ability to prevent such attacks as malware, botnets, viruses	46%
Compatibility with high-level encryption standards	40%
Manageability and usage controls	25%
Security certification and testing	52%
Other (please specify)	2%
Total	257%

Q6. How does your organization determine USB drive reliability and integrity?	Consolidated
Before purchasing, we confirm compliance with leading security standards	49%
Before using, we test to ensure there is no malicious code on these tools	31%
Before using, we test to ensure that data on the device is not corrupted	40%
We only purchase from trusted vendors	37%
We do not test for reliability and integrity	31%
Other (please specify)	3%
Total	190%

Q7. How does your organization prevent low quality, everyday consumer drives from being used in the workplace?	Consolidated
Awareness and training of employees	39%
Creation of a policy	47%
Strict enforcement of the policy	36%
End-user registration of their USB drives	9%
Regular inventory of USB drives	18%
We do not do anything to prevent low quality devices from being used	27%
Other (please specify)	3%
Total	179%

Q8. Does your organization require any of the following security practices to increase the security of USB drives? Please select all that apply.	Consolidated
Use of passwords or locks	43%
Monitor and track USB drives as part of asset management procedures	29%
Deploy encryption for data stored on the USB drive	42%
Scan device for virus or malware infections	31%
Total lockdown through the use of a software solution to block the usage of USB ports	35%
None of the above	46%
Other (please specify)	3%
Total	230%

Part 3. Experience

Q9a. Approximately (best guess), how many USB drives are used by employees (end-users) in your organization today?	Consolidated
Less than 100	3%
100 to 1,000	7%
1,001 to 10,000	14%
10,001 to 50,000	23%
50,001 to 100,000	25%
More than 100,000	10%
Cannot determine	18%
Total	100%

Q9b. Approximately (best guess), what percent of USB drives used by employees (end-users) in your organization are safe and secure?	Consolidated
None	11%
1 to 20%	15%
21 to 40%	18%
41 to 60%	8%
61 to 80%	3%
81 to 100%	46%
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.	Consolidated
Consumer data	21%
Customer data	47%
Employee records	27%
Non-financial confidential documents	40%
Financial confidential documents	17%
Source code	5%
Trade secrets	7%
Other intellectual properties	31%
Other (please specify)	2%
Total	197%

Q11. What types of sensitive or confidential information are normally encrypted when stored on a USB drive? Please check all that apply.	Consolidated
Consumer data	8%
Customer data	41%
Employee records	37%
Non-financial confidential documents	35%
Financial confidential documents	33%
Source code	8%
Trade secrets	30%
Other intellectual properties	26%
We do not encrypt data stored on USB drives (Go to Q13)	34%
Other (please specify)	1%
Total	254%

Q12. What are the two main reasons why your organization encrypts data on USB drives?	Consolidated
Compliance with regulations/EU and nation-specific privacy laws	49%
Comply with self-regulatory programs such as PCI DSS, ISO, NIST and others	38%
Minimize end-user data mishaps resulting from lost USB drives	31%
Comply with vendor or business partner agreements	5%
Avoid harms to customers resulting from data loss or theft	11%
Minimize the cost of data breach	19%
Minimize the affect of cyber attacks	9%
Improve security posture	33%
Other (please specify)	1%
Total	197%

Q13. How important is the requirement that USB drives meet high data security standards? Very important and important (response combined)	Consolidated
Response	77%

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.	Consolidated
Departments/Operating Units	Evaluating USB drives
IT operations	4%
IT security	20%
Business units	34%
Procurement	24%
Compliance & legal	9%
Data center management	7%
Other (please specify)	2%
Total	100%

Departments/Operating Units	Purchasing USB drives
IT operations	15%
IT security	7%
Business units	39%
Procurement	32%
Compliance & legal	1%
Data center management	3%
Other (please specify)	3%
Total	100%

Departments/Operating Units	Purchasing USB drives
IT operations	37%
IT security	2%
Business units	38%
Procurement	3%
Compliance & legal	6%
Data center management	8%
Other (please specify)	6%
Total	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.	Consolidated
Pre stage – IT security has not been established as a program within our company.	8%
Early stage – IT security program is just starting to become staffed and organized.	18%
Middle stage – IT security program is in existence and is starting to launch key initiatives.	39%
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.	12%
Total	100%

Q16. How frequently are USB drives reported as lost or missing in your organization? All the time & very frequently (response combined)	Consolidated
Response	44%

Q17. What procedures are in place to recover or secure missing UBS devices? Please select all that apply.	Consolidated
End-users required to contact help desk immediately	13%
Remote termination of device (kill switch)	8%
Bounty program (finder's fee)	9%
Image backup determines what was on the device	16%
No formal procedures in place to recover lost USB drives	44%
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?	Consolidated
Yes, absolutely certain	31%
Yes, most likely	31%
No (Go to Q20)	31%
Unsure (Go to Q20)	7%
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?	Consolidated
Only 1	37%
2 to 5	23%
6 to 10	20%
More than 10	8%
Cannot determine	12%
Total	100%

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?	Consolidated
Yes, absolutely certain	12%
Yes, most likely	23%
No (Go to Q20)	41%
Unsure (Go to Q20)	24%
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?	Consolidated
Less than 100	36%
100 to 1,000	30%
1,001 to 10,000	10%
10,001 to 50,000	7%
50,001 to 100,001	6%
100,001 to 500,000	4%
500,001 to 1 million	1%
More than 1 million	0%
Cannot determine	6%
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?	Consolidated
None	5%
1 to 20%	3%
21 to 40%	8%
41 to 60%	20%
61 to 80%	20%
81 to 100%	41%
Cannot determine	4%
Total	100%

Q19. Approximately what percentage of missing USB drives are not reported by employees to appropriate authorities in your organization?	Consolidated
None	5%
1 to 20%	5%
21 to 40%	10%
41 to 60%	18%
61 to 80%	23%
81 to 100%	35%
Cannot determine	4%
Total	100%

Q20. Approximately what percentage of missing USB drives result from employee (end-user) negligence rather than fraud, theft or other malicious acts?	Consolidated
None	9%
1 to 20%	7%
21 to 40%	6%
41 to 60%	12%
61 to 80%	18%
81 to 100%	45%
Cannot determine	3%
Total	100%

Q21a. Approximately what percentage of USB drives in use within your organization today are likely to be infected with malware or viruses.	Consolidated
None	15%
1 to 5%	20%
6 to 10%	18%
11 to 20%	10%
More than 20%	6%
Cannot determine	31%
Total	100%

Q21b. Do malware-infected USB drives ever cause the loss or theft of confidential information contained on this device?	Consolidated
Yes	43%
No	44%
Unsure	13%
Total	100%

Part 5. Your role and organization

D1. What organizational level best describes your current position (approximate titles)?	Consolidated
Senior Executive	1%
Vice President	1%
Director	15%
Manager	28%
Supervisor	16%
Technician	26%
Staff	2%
Contractor	7%
Other	6%
Total	100%

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

D3. Check the **Primary Person** you or your IT security leader reports to within the organization.	Consolidated
CEO/Executive Committee	1%
Chief Financial Officer	2%
General Counsel	1%
Chief Information Officer	59%
Compliance Officer	6%
Human Resources VP	5%
Chief Information Security Officer CISO)	11%
Chief Risk Officer	8%
Other	3%
Total	100%

Total years of relevant experience (mean value)	Consolidated
D4a. Total years of IT or security experience	10.75
D4b. Total years in current position	4.67

D5. Gender	Consolidated
Female	31%
Male	69%
Total	100%

D6. What industry best describes your organization's industry focus?	Average
Financial services	19%
Public sector	12%
Services	9%
Consumer products	8%
Industrial	7%
Transportation	7%
Health & pharmaceutical	6%
Communications	5%
Education & research	5%
Entertainment & media	5%
Technology & software	5%
Hospitality	4%
Retailing	4%
Energy	2%
Defense	2%
Total	100%

D7. Where are your employees located? (Check all that apply):	Consolidated
North America	78%
Europe	100%
Middle East & Africa	41%
Asia-Pacific	52%
Latin America (including Mexico)	25%

D8. What is the worldwide headcount of your organization?	Consolidated
Less than 500	16%
500 to 1,000	24%
1,001 to 5,000	27%
5,001 to 25,000	19%
25,001 to 75,000	9%
More than 75,000	4%
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.