

**CREDANT**<sup>®</sup>  
**TECHNOLOGIES**



*Be mobile. Be secure.*

**SURVEY ON  
PORTABLE STORAGE  
DEVICES**

CREDANT Technologies Report  
"iPods – What You Don't Secure  
Could Hurt You"

**Summer 2007**

## TABLE OF CONTENTS

---

### CREDANT Technologies' Survey on Portable Storage Devices "iPods, What You Don't Secure Could Hurt You"

Executive Summary	3-4
Summary of all Findings	5-6
Analysis of Findings	7-19
Conclusion	20
Contacts	20
Methodology	20

An explosion of data-ready phones, USB flash drives, iPods and other portable storage devices has hit the workplace delivering unparalleled mobility, portability and storage capacity. While data mobility has increased worker productivity, the sheer number and small size of storage devices makes them easy to lose or hide. As a result, today's data portability has increased the potential for data leakage, data breaches and identity theft. Until now, data breaches have been caused primarily by lost and stolen laptops. But the popularity of highly portable storage devices; their appeal to Generation X and Y; and their adoption in the workplace, are fueling an increase in risk. According to the Privacy Rights Organization<sup>1</sup>, over 158 million data records of U.S. residents have been exposed due to security breaches since January 2005. Corporate data breaches have been the driving force behind compliance regulations. The growing use of these mini-storage devices without security will only increase the number of security breaches.

CREDANT's survey on portable storage devices sought to discover what security impact these new devices have on the workplace. CREDANT polled 323 respondents, primarily from IT, representing CEOs, CIOs, vice presidents, directors and staff of industries including finance/banking, insurance, healthcare, retail, manufacturing, telecommunications, transportation, state and local government and education. The objective of the survey was to find out if organizations are prepared for future breaches from iPods, whose storage reaches 80 gigabytes, as well as other MP3 players and USB flash drives. The survey respondents were asked a series of questions and their responses are detailed in this report.

Following are the top 5 key findings:

- Not surprising, 86% of those polled cited the USB flash drive as the device most often used to store data exchanged between computers, data-centric phones with SD cards came in second. But when asked to rank these devices as a source of data leakage the iPod is beginning to be viewed as much of a threat as the SD card/smart phone. 13% chose the data-centric phone and, very close behind, 10% said the iPod was the biggest threat to corporate data.
- Adoption of the iPod at work is high with 61% of respondents stating that they use their iPod when traveling or at work. iPods are being brought into the work place by Generation X and Y employees, ages 18 – 40, the average age cited by 92% of respondents. Both generations have grown up with computers. The transition from thinking iPods are simply an audio player will change quickly as more and more of these users consolidate storage devices and learn how easily an iPod or any MP3 player can be used to store large amounts of data.
- There is a lack of understanding as to the threat iPods introduce to an organization. Widely adopted, their data leakage threat is not nearly as well understood as that of the USB flash drive. 61% of respondents had never heard of "pod slurping" — the downloading of corporate data to an iPod—yet 67% of all respondents believe that iPods are a "threat" now. Organizations are faced with the challenge of making sure that all of the data stored on these devices is secured because the issue of data privacy and the requirement to encrypt data applies *to any platform or vehicle* used to store personally identifiable data and an 80 gigabyte iPod can hold a lot of data.
- Despite the fact that 67% of all respondents believe that iPods are a security threat today, 49% stated they would not take any preventative action to protect against potential breaches until they know that the devices are more widely used to store business data on them.

---

<sup>1</sup> [www.privacyrights.org](http://www.privacyrights.org)

- Only 6% of all respondents have an encryption solution for data stored on iPods. 40% have done nothing, and 46% say they have a written security policy governing their use.

Portable storage devices have become pervasive throughout the work place. One of the leading industry research firms estimated that the shipment of USB flash drives would exceed 114 million and SD/CF cards would exceed 375 million by the end of 2006. And Apple has sold over 100 million iPods. These highly vulnerable portable storage devices continue to push the consumerization of IT to the limit. Alarming, people think that iPods pose a threat to their organization, but too few people understand what that threat is. Furthermore, too few organizations are prepared to address the issue.

This survey revealed that the use of iPods is wide spread in organizations today and that little has been done to assess the risk, communicate the threat they pose, or provide security for these devices. The threat of a data breach remains the same irrespective of platform — the issue of data privacy and the requirement to encrypt stored data remains intact and are platform independent. As a result, organizations are highly susceptible to a data breach when any portable storage device containing sensitive data, even an iPod, is lost or stolen. Unfortunately too many will do nothing until they think these devices are being widely used to store business data on them. For heavily regulated organizations, an iPod can be disastrous to a compliance plan that is only executed to secure desktops, laptops and/or USB flash drives. Without security implemented for all mobile devices, organizations remain highly vulnerable to data breaches. Waiting until a VA-type incident occurs to take action will be too late for many organizations.

Read the rest of this report to see all the results and findings from CREDANT Technologies' survey on portable storage devices and learn more about "iPods – What You Don't Secure Could Hurt You."

## SUMMARY OF ALL FINDINGS

- 323 respondents primarily from IT, representing CEOs, CIOs, CISOs, vice presidents, directors and staff of industries including high-tech, finance, healthcare, government, and manufacturing completed the survey. The objective of the survey was to find out what organizations think about the use of iPods and other portable storage devices in the workplace.
- The device most often used for data storage by those polled was the USB flash drive. 86% of those polled see these devices used most often to store data exchanged between computers. Data-centric phones with SD cards were next at 10%, and the iPod was ranked third at 4%.
- When asked to rank these same devices for data leakage, the iPod is beginning to be viewed as being as much of a threat as the SD card/smart phone. 78% said the USB flash drive is the greatest threat to organizations, 13% chose the data-centric phone and very close behind, 10% said the iPod was the biggest threat to corporate data.
- When asked if the iPhone would pose a threat to their organization, 58% said it would increase the risk of data leakage while 15% said it would not be a threat. Most said it would be as much of a threat for data leakage as any smart phone or iPod with storage. However, almost all of those who said the iPhone would not be a threat, also stated that their organization was not going to support it as an approved company device.
- iPod adoption within the workplace is high: 61% of all respondents use them when traveling or at work. Of those who don't use one, a high percentage state they are not allowed at work, they don't own one, or they use another device. This, coupled with their estimation of the overall adoption within the work place, should be an eye-opener for security administrators.
- Asked when they use their iPods at work, 35% of respondents stated while on breaks; 57% when traveling for business; 30% use them to drown out noise while working; and 7% use them to store business data.
- iPods brought into the workplace have been driven by Generation X and Y, ages 18 - 40. 59% of respondents cited that the average age of those using iPods ranges from 18 to 30 years of age, with the age range of 31 to 40 coming in second place at 33%. Total use by Generation X and Y = 92%.
- When asked why an iPod might be used to store data, the number one reason given by 55% of respondents was to reduce the number of devices one has to carry. 51% stated that it is as easy to use as any external drive to store business data.
- When asked if they knew what pod slurping is (the downloading of data onto such a device with the intent to steal it or copy it without a right to do so), 61% were not aware of the term; 33% had heard of it; and 5% had seen it in action.
- The poll asked respondents when they thought iPods would become a security threat to their organizations. 67% said they already are! 11% stated one year and 12% said they would become a threat in the next two years. 7% stated they never would become a threat.

## SUMMARY OF ALL FINDINGS cont.

---

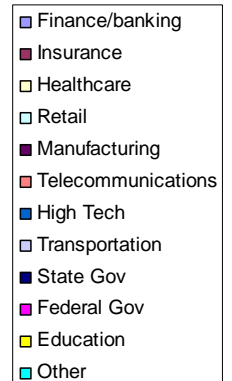
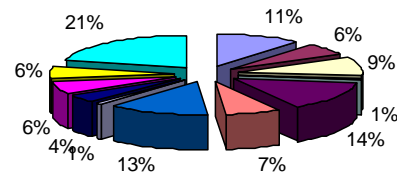
- 40% of respondents stated that no security measures have been put in place to prevent data breaches on iPods and other portable storage devices. 46% of organization representatives say they have written policies in place and 12% stated that they use security software of some type to stop data leaks.
- Alarming, too few people understand the threat iPods introduce to an organization and too many organizations (49%) are not prepared to address the issue. As a result, organizations are highly susceptible to a data breach when one of these devices is lost or stolen. Unfortunately too many will do nothing until they think they are being widely used to store business data on them.
- 79% of respondents stated that every day they work with data that, if lost, by law would require their organization to publicly notify potential victims. The notification process is costly and can deeply scar an organization's reputation, as evidenced in the publicized laptop data thefts and losses in recent months.

323 respondents primarily from IT, representing CEOs, CIOs, CISOs, vice presidents, directors, and staff of industries including high-tech, finance, healthcare, government, and manufacturing completed the survey. The objective of the survey was to find out what organizations think about the use of iPods and other portable storage devices in the workplace.

**Role of Survey Participants**



**Industries Represented**

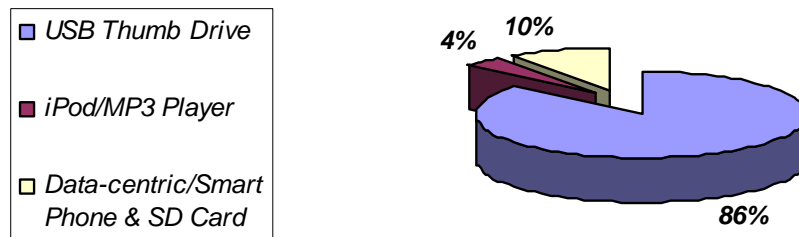


CREDANT polled 323 respondents, primarily from IT, representing CEOs, CIOs, CISOs, vice presidents, directors and staff of industries including high-tech, finance, healthcare, government, manufacturing and others. The objective of this survey was to find out if organizations are aware of the potential impact of new types of storage devices on future data breaches. IT staff made up the greatest majority of the "other" category within the role of survey participants. Within IT staff, the respondents were a mix of security, network administration, IT auditors, technical architects, and support.

**Questions 16 & 17:** *What is your role within the organization? What industry do you work in?*

The device most often used for data storage by those polled was the USB flash drive. 86% of those polled see these devices used most often to store data exchanged between computers. Data-centric smart phones with SD cards were next at 10%, and the iPod was ranked third at 4%.

### **Ranking of External Storage Devices Most Often Used Today**

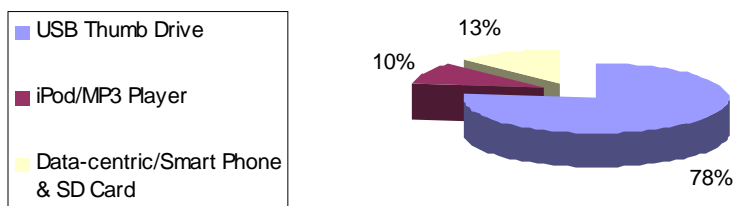


When assessing the risk posed by three types of devices – USB flash drives, iPod/MP3 players and data centric/smart phones and SD cards, respondents were first asked which device is used the most for data storage. 86 % of respondents stated they use USB flash drives most frequently. These devices are often in large supply, inexpensive, and are given away at trade shows. The next most often used devices for storage were smart phones equipped with SD cards at 10%. And a potential up and coming threat, but still not used primarily as a data storage device, were iPods/MP3 players at 4%. The comments revealed that respondents were aware that all of these devices could be used to store business data.

**Question 1:** Many new types of devices are being used to store business data that moves within and outside of an organization. Please rank the following devices based on how often you think they are used to store business data. 1 having highest usage - 3 having the lowest usage. (Choices were USB drive, iPod/MP3 player, data-centric/smartphone & SD Card)

When asked to rank these same devices for data leakage the iPod is beginning to be viewed as being as much of a threat as the SD card/smart phone. 78% said the USB flash drive is the greatest threat to organizations, 13% chose the data-centric phone and 10% said the iPod was the biggest threat to corporate data.

**Ranking of External Storage Devices Based on Perceived Security Threat**

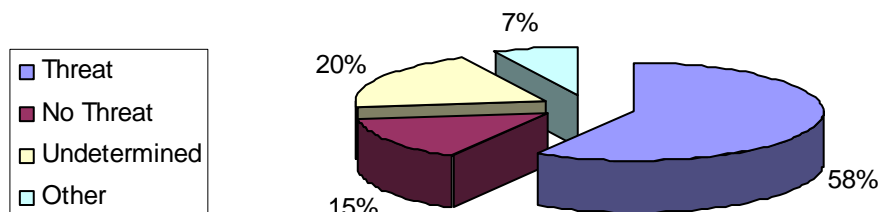


It is no surprise that more than three-quarters (78%) of respondents stated that USB flash drives used in the workplace are the greatest threat to data leakage today. They are everywhere, can cost less than \$15 or \$20 each, and are given away at trade shows and events. But, the respondents' answers show that the iPod is beginning to approach the same level of perceived threat as SD cards/data-centric smart phones. Those polled ranked the threat of data loss via a data-centric smart phone at 13% and via the iPod at 10%. This third-place rating is just the start of something bigger; with their growing adoption, the prevalence of iPods used as storage devices will only continue to increase. Several respondents stated that the iPod allows them to carry just one storage device whether at home or in the office.

**Question 2:** *Organizations are very concerned about data leakage and the threat of a data breach when a portable device that contains personal information is lost or stolen. Please rank the following devices based on what you believe their threat is to an organization. 1 being the highest threat, 3 the lowest threat. (Choices were USB drive, iPod/MP3 player, and data-centric/smart phone & SD card)*

When asked if the iPhone would pose a threat to their organization, 58% said it would increase the risk of data leakage; 15% said it would not be a threat. Most said it would be as much of a threat for data leakage as any smart phone or iPod with storage. However, almost all of those who said the iPhone would not be a threat also stated that their organization was not going support it as an approved company device.

### ***Impact of iPhone on Data Leakage***



With over 700,000 iPhones sold the first weekend they were available, the security concern highlighted by respondents is valid. Concern around the arrival of the iPhone, even at its high price point of \$599.99 for an 8GB device, brought a flurry of mostly wary comments — executives and IT managers polled realize the iPhone is as much a threat for data leakage as any other smart phone, USB drive, or iPod. 58% of respondents said the iPhone will have an impact on data leakage. 15% said it would not have an impact, but based on the respondents' comments, many of those say the iPhone won't be a threat because their workplace won't be certifying it as an "allowed" or supported company device and therefore they expect it to be less prevalent in their particular workplace.

**Question 3:** *Do you think the new iPhone will have an impact on data leakage?*

**Comments:**

*"Highly likely. With the device being consumer-centric and connection-friendly, and with the vast amount of storage space available, the iPhone is an ideal candidate to store files for transport."*

*"It will reduce data leakage because you will reduce at least by two the number of devices you can lose."*

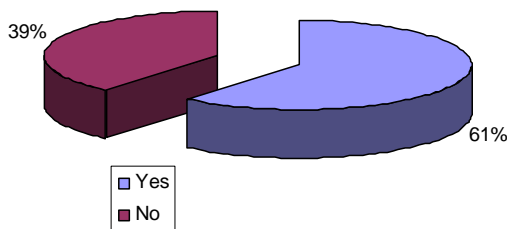
*"I think any storage device that can be portable with little governance over it can have a major impact on the company if it's in the wrong hands."*

*"Any device that offers large amounts of storage, is new technology and not clearly understood will offer new avenues to data leakage."*

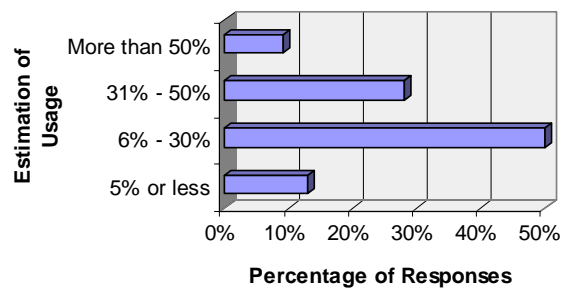
*"No—they are not authorized to be purchased under our existing cellular provider agreement."*

iPod adoption within the workplace is high: 61% of all respondents use them when traveling or at work. Of those who don't use one, a high percentage state they are not allowed at work, they don't own one, or they use another device. This, coupled with their estimation of the overall adoption rate within the workplace, should be an eye-opener for security administrators.

**iPod Usage at Work by Respondents**



**Estimation of iPod Adoption in the Work Place**



Apple has sold more than 100 million iPods, and it is not surprising that many of them have been brought to the office. What is surprising is how rapidly they have penetrated the work environment. 61% of respondents have an iPod and use it while at work or traveling on business. This is higher than one might expect or be prepared to deal with from a security perspective. When asked to estimate the percentage of people they thought used iPods or MP3 players, 50% of respondents believed that more people are beginning to use these devices and that an average of 6% - 30% of all employees have one. 28% of respondents felt the adoption rate was between 31% - 50% of all employees; only 9% believed that nearly everyone at their office had an iPod or MP3 player. Even a large majority of those who said, "No, I do not use an iPod at work", stated that it was because they were told not to bring it to work. The use of iPods and MP3 players at work cannot be ignored. The potential data leakage impact of these devices must be assessed by each organization – and sooner rather than later.

**Question 4:** *Do you ever use your iPod/MP3 player at work or while traveling on business?*

*Yes; No - why don't you use it at work?*

**Question 6:** *What percentage of people do you think use iPods or MP3 players at work or when traveling on business?*

*5% or less; 6% to 30%; 31% to 50%; More than 50%*

**Comments:**

*"I store MP3's on my computer and use that."*

*"I only use it during travel, but for music only."*

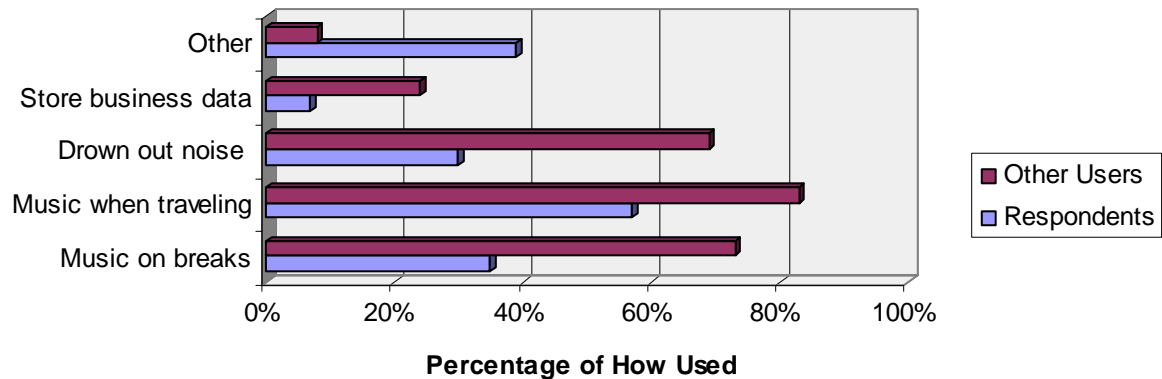
*"Not allowed."*

*"Against company policy."*

*"Don't have one."*

Asked when they use their iPods at work, 35% of respondents stated while on breaks; 57% when traveling for business; 30% use it to drown out noise while working; and 7% use them to store business data.

### How iPods and MP3 Players are Used at Work



The iPod has definitely found a place in the lives of workers both on and off the job. More than half of the respondents (57%) use one to listen to music when traveling on business, with 35% adding they use it on breaks, and 30% stating they use an iPod/MP3 player to drown out noise. When asked how they felt others used these devices, the percentages of how they were used increased, but the way they were used remained constant — for music when on breaks or traveling and to drown out noise. What did increase was the percentage that use the device to store business data —from 7% to 24%. In the Comments section, many respondents identified that they use their iPod as an audio learning tool. While only a small percentage (24%) say they transfer corporate data to their iPod today, that number equates to a huge potential for data loss in large corporations or when the number is multiplied by the number of iPods that are brought into the workplace.

**Question 5:** *What do you use the iPod/MP3 at work for? Please check all that apply.*

**Question 8:** *What do they (other employees) use the iPod/MP3 at work for?*

*I use it on breaks to listen to music; I use it when traveling on business to listen to music; I use it when working on projects to help drown out noise; I use it to store business data.*

**Comments:**

*"I use it while commuting to and from work."*

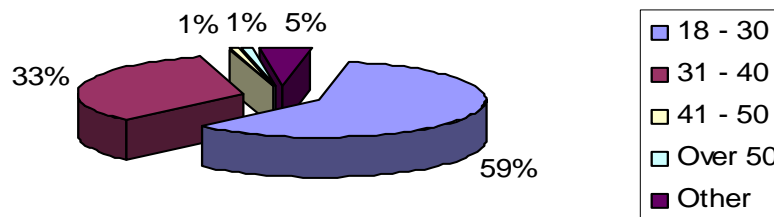
*"I use it to listen to music and podcasts in my car."*

*"Audio learning."*

*"I listen to podcasts of business meetings and training sessions."*

iPods brought into the workplace have been driven by Generation X and Y, ages 18 – 40. 59% of respondents cited that the average age of those using iPods ranges from 18 to 30 years, with the age range of 31 to 40 coming in second place at 33%. Total use by Generation X and Y = 92%.

### Average Age of People that Use an iPod at Work



Generation X and Y are driving the use of the iPod within the workforce. Therefore, it was no surprise to see that most of those polled (92%) chose the age ranges between 18 and 40 as the ages of most iPod users. These generations have grown up with computers and the transition from thinking iPods are simply an audio player will change quickly as more and more users consolidate storage devices and learn how easily an iPod or any MP3 player can be used to store large amounts of data. In addition, as organizations use this type of device as education and training tools, the age gap will disappear.

**Question 7:** *What is the average age of the people that use an iPod/MP3 player at work or while traveling for business?*

*18 – 30 years old; 31 – 40 years old; 41 – 50 years old; Over 50; Other, please comment*

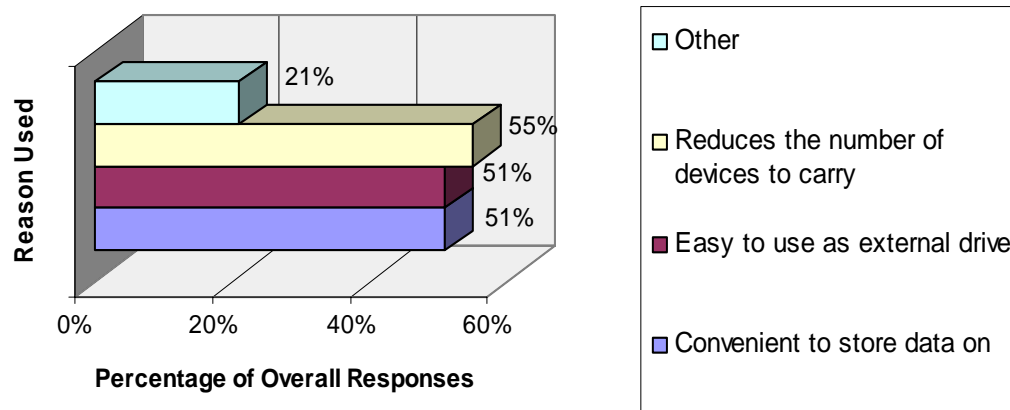
**Comments:**

*"I think it transcends age groups."*

*"I know people in all of these age categories."*

When asked why an iPod might be used to store data, the number one reason given by 55% of respondents was to reduce the number of devices one has to carry. 51% stated that an iPod is as easy to use as any external drive to store business data.

### Reasons Why the iPod is Used to Store Data



The respondents were asked why they thought an iPod would be used to store data. The number one reason chosen by 55% of the respondents was because it reduces the number of devices one has to carry. 51% said that it is as easy to use as any external drive, and another 51% said it is easy to store data on. Many respondents commented that using an iPod to store data is not something they see much of. Others said they use it to store podcasts of meetings and training sessions.

**Question 9:** If you or anyone you know uses their iPod/MP3 player to store business data, why do you think this device is being used? Please check all that apply.

*It is convenient to store data on; It is easy to use as an external drive on any computer; It reduces the number of portable devices we carry around that can store data; Other, please comment.*

#### Comments:

*"It simplifies life."*

*"Use for podcasts of meetings, training sessions, etc."*

*"It's easy and avoids security checks."*

*"It is a combined phone, PDA, and MP3 player."*

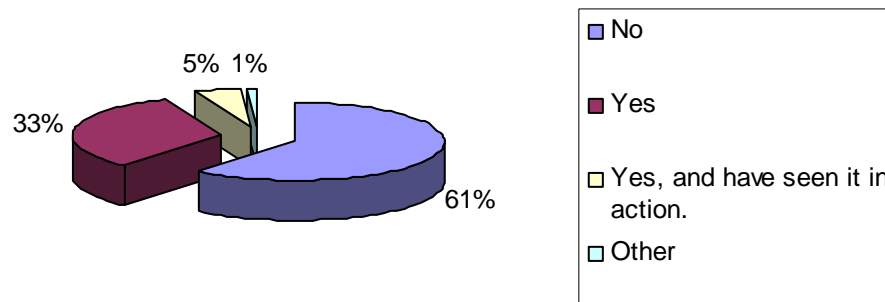
*"USB devices are cheaper, iPods are not."*

*"Better not be using these devices for business!"*

*"Due to policy, they are not used to store data."*

When asked if they knew what pod slurping is (the downloading of data onto such a device with the intent to steal it or copy it without a right to do so), 61% were not aware of the term, 33% had heard of it, and 5% had seen it in action.

### Enterprise Awareness of Pod Slurping



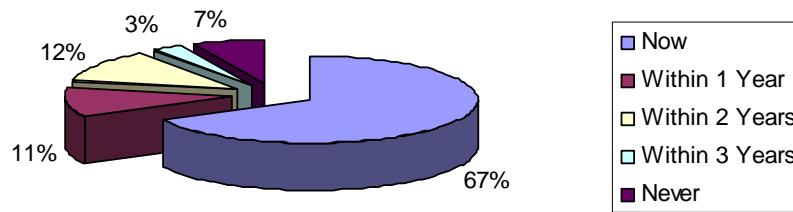
There is a lack of understanding as to the threat iPods introduce to an organization. Organizations are faced with the challenge of making sure that all data stored on these devices is secured. The issue of data privacy and the requirement to encrypt data applies to any platform or vehicle used to store personally identifiable data and an 80 gigabyte iPod can hold a lot of data. Widely used within organizations, their data leakage threat is not nearly as well understood as that of the USB flash drive. 61% of respondents had never heard of “pod slurping” (the downloading of corporate data to an iPod). This answer is not surprising in that iPods are viewed as innocent devices used to listen to music or podcasts when traveling on business, or on break, or to drown out noise in the office. Currently, USB flash drives are the least expensive storage device and the most commonly used vehicle to transfer and store corporate data. But that will change quickly as more and more business users realize that the iPod, in addition to playing music, is an external storage device that can be used with any computer and can reduce the number of devices they carry around and potentially lose.

**Question 10:** *Are you aware of “pod slurping”?*

*No, I haven't heard of this term before; Yes. Pod slurping is the downloading of corporate data to an iPod and removing it from the office; I have heard of pod slurping and have seen it in action; Other, please comment.*

The survey asked respondents when they thought iPods would become a security threat to their organizations. 67% said they already are! 11% stated within one year and 12% said they would become a threat in the next two years. 7% stated they never would become a threat.

**When iPods Will Pose a Security Threat to Enterprises**



The survey highlighted the lack of understanding as to what threat iPods pose to an organization when 61% of respondents had never heard of "pod slurping" (the downloading of corporate data to an iPod). Yet, when asked when they thought the iPod/MP3 player would become a security threat to their organization, 67% of all respondents believe that they are a threat now and only 7% believe they will never be a threat. One respondent summarized the sentiments of many; "While it's convenient to use it to store other data, most users probably would know how to use it to upload music files and to use it as an MP3/music player only."

Generation X and Y, have grown up with computers and the transition from thinking iPods are simply an audio player will change quickly as more and more users consolidate storage devices and learn how easily an iPod or an MP3 player can be used to store large amounts of data. Using an iPod as a storage device is as simple as plugging it in to the USB port of a computer where it is recognized as an external hard drive. From this point on, the user can simply drag and drop any files to the iPod and easily exchange that data between computers by plugging in the device and transferring the data.

This problem will only snowball as the iPhone and other converged devices with larger storage capacity and wireless connectivity become prevalent within the workplace. Downloading files from the corporate network will be even easier then: nothing will have to be plugged in because files will simply be exchanged wirelessly. In order to be in compliance, organizations will have to stay abreast of all new devices.

**Question 11:** *When do you think iPods/MP3 players will become a security threat to your organization or any organization? They already are; Within 1 year; Within 2 years; Within 3 years; Never*

**Question 12:** If you answered Never to question 11, why do you believe iPod/MP3 players will not become a security threat to an organization?

**Comments:**

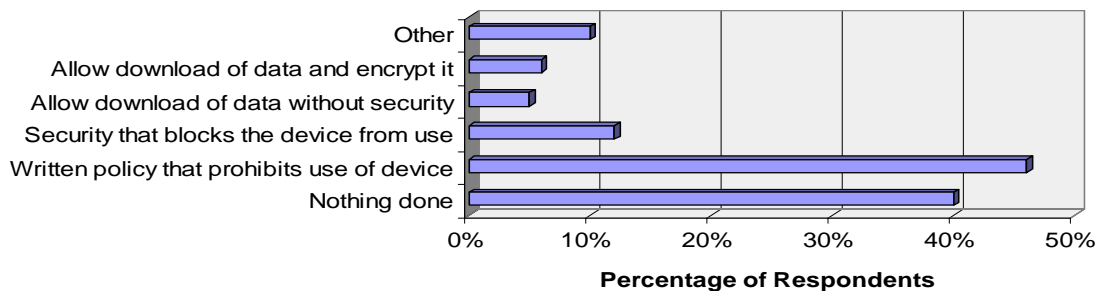
"I personally don't want to expose my iPod to any corporate policies. It's a personal device and I don't want 3rd party control over it. Anyway, thumb drives are tiny and not a problem to carry in your pocket."

"If the company sets up their security properly, there will be no issues."

"They are too slow and not good for much outside of music really."

40% of respondents stated that no security measures have been put in place to prevent data breaches on iPods and storage devices from happening. 46% say they have written policies in place. 12% stated that they use security software of some type to stop data leaks.

### Security Measures Implemented



The survey highlights a potentially serious gap in many organizations' security strategy. Even though 67% of respondents feel iPods are a threat today, only 12% of the respondents stated that security measures have been implemented. 40% have nothing in place and 46% have a written policy. Enterprises can no longer take chances with the number of new small storage devices that are entering the workplace. The convenience of mobility is negated by seemingly innocent devices that can undermine an organization's security and compliance, as highlighted in this survey. Based on responses to the survey, organizations are clearly not prepared for the iPod. 86% of all respondents stated that the iPod/MP3 players have not been secured even though they think these devices are a threat. Why? The iPod is thought of as a harmless device that is used by many employees while traveling on business, or to drown out distracting noise while working on projects, or to simply relax and enjoy music while on break. Alarming, too few people understand the threat iPods introduce to an organization. Furthermore, any new device that can store data will have to be considered a threat because no matter how innocent the device appears, if personally identifiable or other sensitive data is stored on it when it vanishes, the liability for compliance falls on the shoulders of the organization.

**Question 13:** *What security measures has your organization implemented to prevent employees from storing business data on iPods/MP3 players? Please check all that apply.*

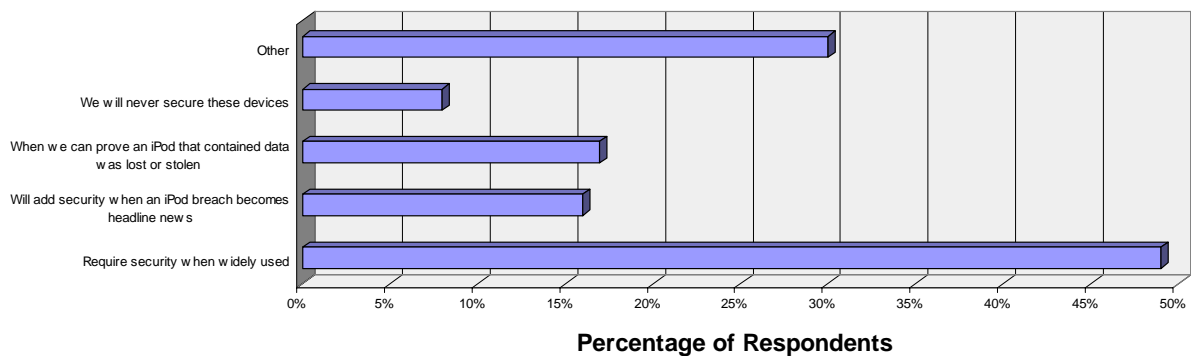
*Our organization has not done anything yet; We have a written security policy that prohibits use of such devices but do not enforce the policy with software; We have security software that blocks the device from being used; We allow someone to download data to these devices but do not secure the device; We allow someone to download data to these devices but ensure that the data is encrypted; Other, please comment.*

#### Comments:

- "Users must abide by the Acceptable Usage policy"*
- "Policy regarding mobile data"*
- "Organizations are now putting a ban on these devices"*
- "As policy, they are not allowed a network connection"*
- "Security policy addresses proper use of data"*

Alarming, too few people understand the threat iPods introduce to an organization and too many organizations (49%) are not prepared to address the issue. As a result, organizations are highly susceptible to a data breach when one of these devices is lost or stolen. Unfortunately too many will do nothing until they think these devices are being widely used to store business data.

**When Will Enterprises Take Action to Secure iPods**



Too few people understand the threat iPods introduce to an organization or understand the population of employees who are bringing iPods into the workplace. Question 4 highlighted the fact that 61% of all respondents to the survey have their iPod with them while working. When respondents were asked when their firms would begin to move toward implementing a security solution, the highest percentage, 49% stated, "When we think they are being widely used to store business data on them." 17% said "We will add security if and when we can prove a device that contained business data was lost or stolen." 16% actually responded, "We will add security when we see organizations in the newspaper headlines because of a lost or stolen iPod/MP3 player." Although many respondents stated that they are beginning to assess the problem, create a policy for these devices or are evaluating security software, too few are heeding the warning signs.

**Question 14:** *If your organization has not implemented security measures for iPod/MP3 players, when do you think they will do something? Please check all that apply.*

*We will require security when we think they are being widely used to store business data; We will add security when we see organizations in the newspaper headlines because of a lost or stolen iPod/MP3 player; We will never enforce security on them because they are personally owned devices; Other, please comment.*

**Comments:**

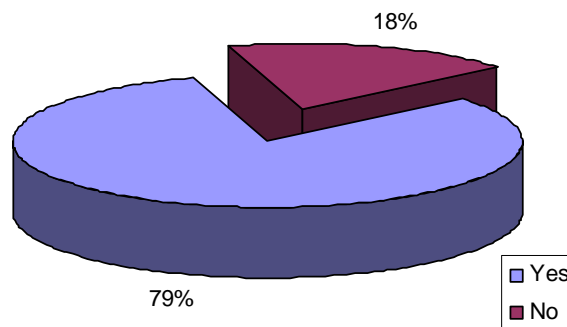
"I worry."

"Will limit external drives of all kinds this year."

"Don't think it will be a problem."

79% of respondents stated that every day they work with data that, if lost, by law would require their organization to publicly notify potential victims. The notification process is costly and can deeply scar an organization's reputation, as evidenced in the publicized laptop data thefts and losses in recent months.

**Percentage of Respondents that Work for Organizations that Handle Sensitive Data**



The probability of a data breach caused by the proliferation of iPods/MP3 players and USB flash drives within the workplace has increased dramatically. 79% of the respondents stated that they work with data that, by law, would require their organization to publicly notify any potential victims if the data were lost or stolen. With the number of small, highly portable storage devices in the workplace, it is just a matter of time before a breach occurs when one of these devices is lost or stolen. One of the leading industry research firms estimated that the shipment of USB flash drives would exceed 114 million and SD/CF cards would exceed 375 million by the end of 2006. And Apple has sold over 100 million iPods. These highly vulnerable portable storage devices continue to push the consumerization of IT to the limit, but the threat of a data breach remains the same irrespective of platform. The issue of data privacy and the requirement to encrypt stored data remains intact and is platform independent. Without security implemented for all mobile devices, organizations remain highly vulnerable to data breaches—and waiting to take action until a VA-type incident occurs will be too late for many organizations.

**Question 15:** *Does your organization handle data that if lost could lead to compliance issues and customer notification?*

Yes; No; Other, please comment.

## CONCLUSION

CREDANT Technologies' Survey on Portable Storage Devices – Summer 2007 found that despite acknowledgement that USB flash drives, iPods/MP3 players and data-centric phones with SD cards are moving into the workplace there is still a reticence to acknowledge or secure these devices. As enterprises, government agencies, schools, and hospitals look for a way to control data leakage from desktops, laptops, USB flash drives, and even iPods, there is a clear need to keep track and secure all devices carrying data. This not only helps an organization better manage data assets, it also ensures that compliance has been met when a device carrying corporate data, or a customer's or patient's identifying information vanishes. Even the possibility that an employee's lost device has leaked data such as social security numbers, addresses, medical histories, or financial information is grounds for notification costs, and financial penalties, and could cause a hailstorm of compliance issues and lawsuits. As in the VA case and others, an organization's reputation and business are at stake.

All organizations will find it almost impossible to stop the use of these highly portable storage devices, but they can take positive steps to ensure that business data stored on them is encrypted when lost or stolen. Software exists today that can control the use of all computing and storage devices while enforcing strong policy-based encryption on the devices to protect data when they disappear.

General inquiries:  
Mary Van Zandt  
CREDANT Technologies  
mvanzandt@credant.com  
972-458-5408

Media inquiries:  
Karin Taylor  
Trainer Communications  
[cd@trainercomm.com](mailto:cd@trainercomm.com)  
408-920-0585/408- 979-0891

## METHODOLOGY

The survey was officially launched in May 2007. Email invitations were sent to 17,000 Global 2000 professionals worldwide, and they were given until the June 8 to participate in the survey. 323 people qualified for and completed all the survey questions. The results of this survey are based on the responses of these individuals. Each respondent was eligible to win a free TOMTOM ONE Portable Car GPS Navigation System.

## ABOUT CREDANT

CREDANT® Technologies is the market leader in mobile data protection solutions. CREDANT's secure mobility solutions preserve customer brand and reduce the cost of compliance, enabling business processes to quickly and safely "go mobile." CREDANT Mobile Guardian is the only centrally managed mobile data protection solution that provides strong authentication, intelligent encryption, usage controls, and key management that guarantees data recovery. By aligning security to the type of user, device and location, CREDANT ensures the audit and enforcement of security policies across all mobile end-points. Strategic partners and customers include leaders in finance, government, healthcare, manufacturing, retail, technology, and services. CREDANT was selected by Red Herring as one of the top 100 privately held companies and top 100 Innovators for 2004, and was named Ernst & Young Entrepreneur Of The Year® for 2005. Austin Ventures, Menlo Ventures, Crescendo Ventures, Intel Capital and Cisco Systems are investors in CREDANT Technologies. For more information, visit [www.credant.com](http://www.credant.com).