# Security of Voice Data

Benchmark study of IT & IT Security Practitioners

Independently Conducted by Ponemon Institute LLC

30 April 2010

# Security of Voice Data

Ponemon Institute 30 April 2010

## I. Executive Summary

*The Security of Voice Data study* was conducted by Ponemon Institute and sponsored by Cellcrypt. Our study attempts for the first time to put an economic cost on the loss of voice data due to cell phone interception. With recent news demonstrating the vulnerability of cell phone calls, it also serves as a wake-up call to those responsible for risk management and IT within organizations to add the insecurity of voice data to their list of possible threats.

According to the findings, 67 percent of IT practitioners surveyed are not confident that the proprietary and confidential information conveyed during cell phone conversations is adequately secured. Further, only 14% of respondents say their organizations use technologies to secure cell phone communications when employees travel to regions they believe pose the greatest risk to voice data. The study also reveals that every time a corporate secret is revealed to unauthorized parties, especially competitors and their agents, it costs the organization an average of $1.3 million.

Seventy-five companies participated in this benchmark study with 107 interviews completed. Our study utilizes a confidential and proprietary benchmark method.

We believe this research on the vulnerability of cell phones is timely because of the December incident involving the cracking of GSM mobile phone call security. As was widely reported in the *New York Times, Wall Street Journal* and other news outlets, hackers put the GSM codebook on the Internet making it available to anyone interested in cracking GSM mobile phone calls. The hackers described the equipment needed to intercept and crack live GSM calls, thus showing that 80 percent of the world's mobile voice calls are at risk.

### Attributions about the security of voice data

This study seeks to understand the level of awareness that highly experienced IT or IT security practitioners have about voice data security and how important to their organizations they see the security of cell phone communications. We asked respondents questions about whether they agree or disagree that their organizations' employees are careful about communicating sensitive information when using cell phones, whether they agree that their policies forbid the use of cell phones for confidential conversations, if existing security features are sufficient and if their cell phone communications are targeted by criminals or spies. Table 1 summarizes the strongly agree and agree responses for individuals participating in our study.

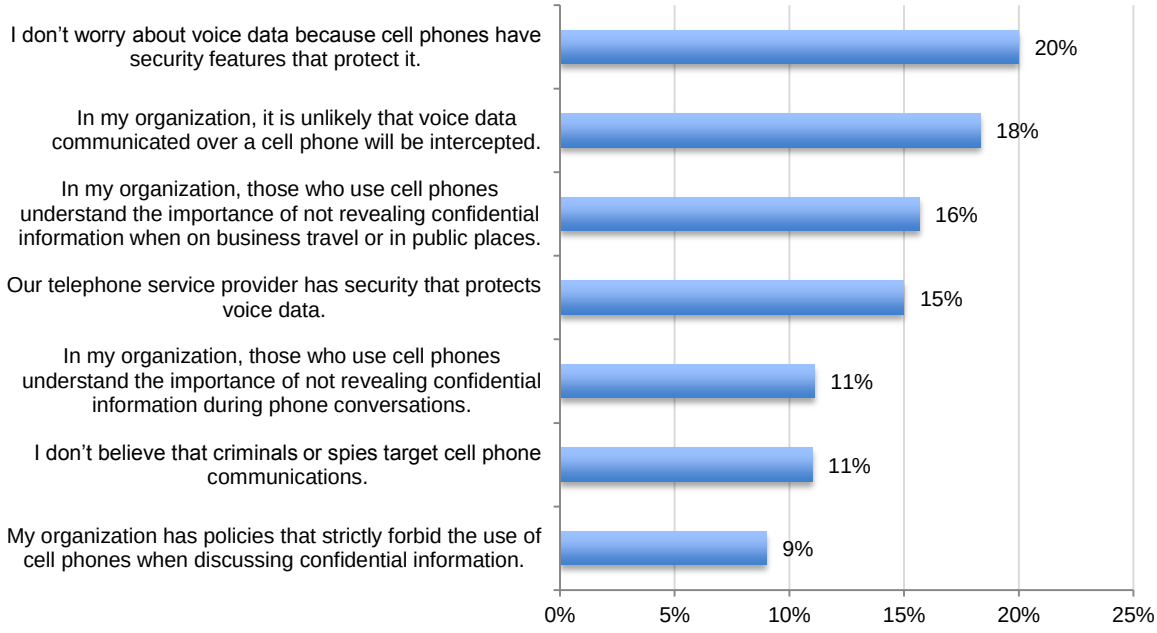
| Table 1: Attributions about the security of voice data | Ex ante | Ex post |
|---|---|---|
| My organization has policies that strictly forbid the use of cell phones when discussing confidential information. | 28% | 19% |
| I don't believe that criminals or spies target cell phone communications. | 46% | 35% |
| Our telephone service provider has security that protects voice data. | 48% | 33% |
| I don't worry about voice data because cell phones have security features that protect it. | 49% | 29% |
| In my organization, those who use cell phones understand the importance of not revealing confidential information during phone conversations. | 52% | 41% |
| In my organization, those who use cell phones understand the importance of not revealing confidential information when on business travel or in public places. | 57% | 42% |
| In my organization, it is unlikely that voice data communicated over a cell phone will be intercepted. | 59% | 41% |

We divided respondents randomly into two groups. The ex ante group completed these seven attributions before reviewing six scenarios in the survey instrument. The ex post group completed the same attributions immediately after reviewing scenarios.

We learned that those who responded to attribution questions at the beginning of the survey (a.k.a. ex ante respondents) were more likely to agree that a serious risk to voice data did not exist in their organizations. In contrast, the respondents who answered at the conclusion (a.k.a. ex post respondents) were more likely to believe that the risk is real and that cell phone communications are at risk.[1] This suggests that the survey questions and scenarios informed participants and increased their awareness of the threats to voice data.

Bar Chart 1 reports the ex ante and ex post differences for seven attributions. As can be seen, all differences are positive, thus suggesting respondents' learned about the issue in the process of completing the survey instrument. The most significant difference (Diff = 20%) concerns the attribution "I don't worry about voice data because cell phones have security features that protect it." The second largest difference (Diff = 18%) concerns the attribution "In my organization, it is unlikely that voice data communicated over a cell phone will be intercepted.

Bar Chart 1: Ex ante ex post differences on seven attributions about the security of voice data



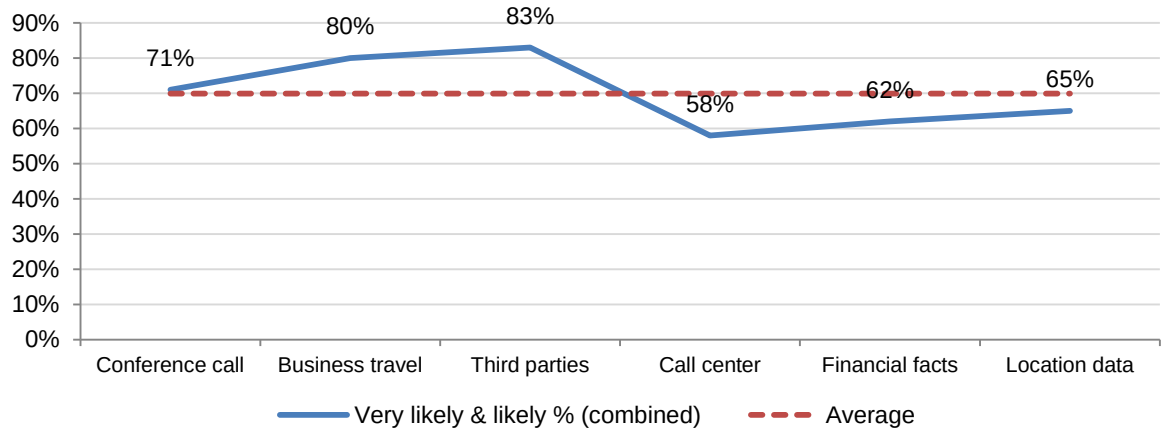

[1] Please note that respondents were randomly assigned to each group.

**Scenarios concerning voice data at risk**

The survey asked participants to respond to the likelihood of six separate scenarios involving the use of cell phones to communicate sensitive and confidential information occurring in their organizations. A summary of these scenarios is provided in Table 2.

| Table 2: Six cases studies where voice data may be at risk |
|---|
| **Conference Call**: An executive relies on his cell phone to participate in conference calls with other senior leaders in the company. During these calls, proprietary and confidential information about the company is sometimes exchanged. |
| **Business travel**: A sales manager who travels extensively to China and other Asian countries uses her cell phone to communicate with the home office in the United States to coordinate sales strategy, pricing and contract information. During these calls, proprietary and confidential information is exchanged. |
| **Third parties**: An outside lawyer contacts his client and requests proprietary and confidential information while using his cell phone. This requested information is provided by an employee over the phone. |
| **Call center**: A customer contacts a company's call center to establish a new account. The information required from the customer includes her name, address, Social Security number and other personal facts. This confidential information is conveyed to the call center over a cell phone. |
| **Financial facts**: A company's finance and accounting staff has a conference call discussing a preliminary press release about quarterly earnings. One of the participants of the call is on a cell phone. |
| **Location data**: A company's chief executive travels to another country to hold merger negotiations with the CEO and board of a major competitor. His administrative assistant uses a cell phone to arrange the CEO's ground transportation, which reveals the identity of the acquisition target. |

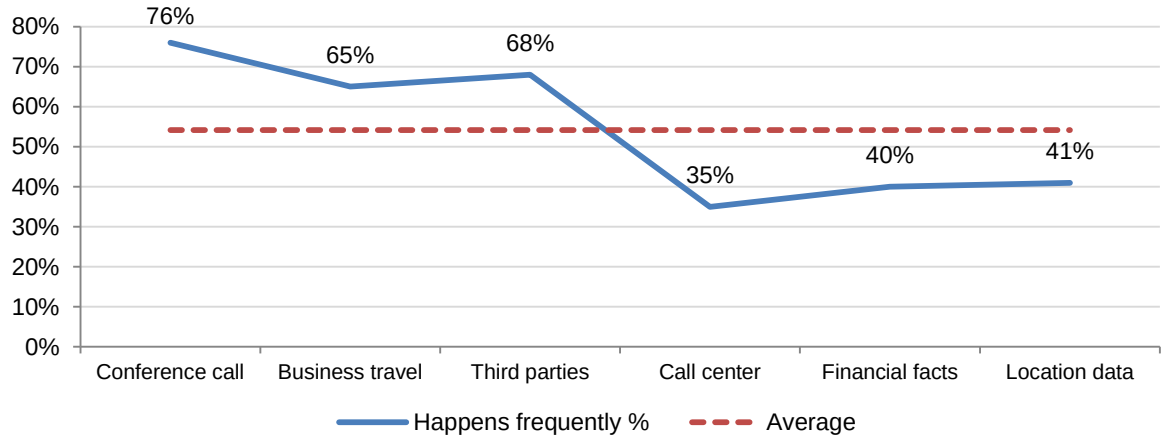
Line Graph 1: The "likely" and "very likely" response (combined) for each scenario




The findings reveal that the most likely scenarios to occur are the outside lawyer asking for proprietary and confidential information using his cell phone (83 percent of respondents), The sales manager in Asia using a cell phone to communicate with the home office (80 percent) and the executive who relies on his or her cell phone to participate in conference calls with other senior leaders of the organization (71 percent). The least likely scenarios to occur are the

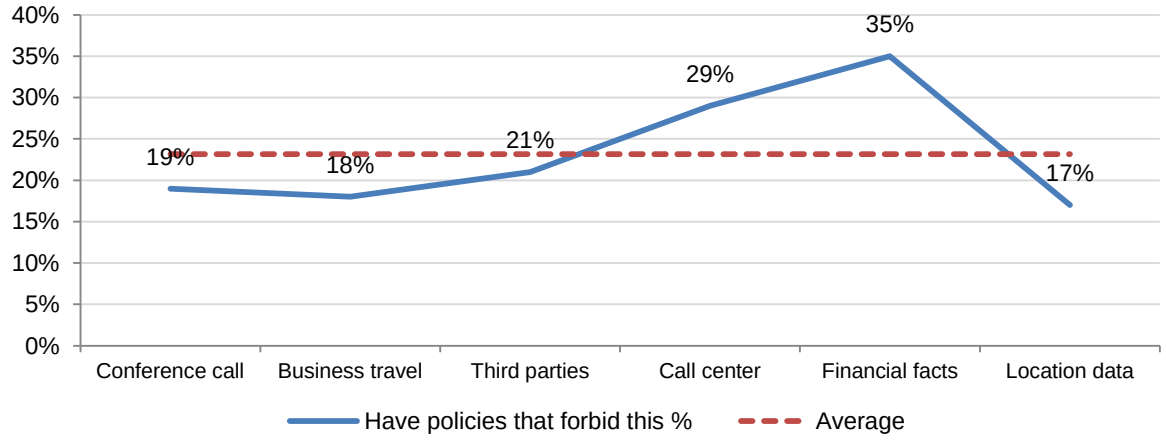
discussion of an earnings release (62 percent) and the call center's collection of a customer's personal information (58 percent).

Line Graph 2: This "happens frequently" response to the issue contained in each scenario




The most prevalent of the practices described in the scenarios involve the senior leaders having a cell phone conversation (76 percent), the outside lawyer (68 percent) and the sales manager in Asia (65 percent). The least prevalent practice is the earnings release and the call center scenarios (40 percent and 35 percent, respectively).

Line Graph 3: Percentage of respondents who say their organization have policies that forbid the issue contained in each scenario




The percentage of companies having policies that forbid the practices described in the scenarios is very low. The highest (35 percent of respondents) concerns the earnings release. This could be attributed to Sarbanes-Oxley regulatory requirements. The lowest (17 percent) concerns the disclosure of the location of the CEO traveling abroad.

## II. Key Findings

Following are the key findings of our study. We illustrate many of these findings in charts or tables based on the percentage frequency of respondents.

### 1. The interception of corporate secrets during cell phone conversations is costly and not likely to be discovered.

The average extrapolated cost to an organization every time a corporate secret is revealed to unauthorized parties, especially agents and their competitors, is estimated at $1.3 million. As shown in Bar Chart 1, 47 percent of respondents believe the cost is more than $1 million.

Bar Chart 1: The average cost organizations incur every time a valuable corporate secret is revealed to unauthorized parties, especially competitors or their agents.

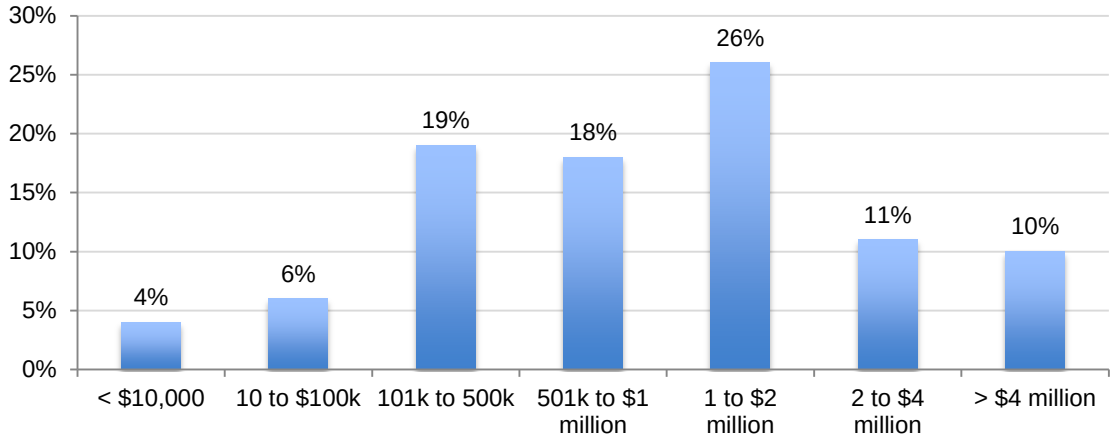



Table 3 shows 43 percent of respondents believing that, on average, a corporate secret is wrongfully obtained about once every month. Twenty-nine percent believe it happens less frequently (about once a year). Only 5 percent state that this type of incident never happens.

| Table 3: How frequently is a corporate secret revealed to unauthorized parties each year? | Pct% |
|---|---|
| About once each year | 29% |
| About once every month | 43% |
| About once every week | 11% |
| About once every day | 7% |
| Never happens | 5% |
| Can't guess | 5% |
| Total | 100% |

| Table 4: How do unauthorized parties obtain corporate secrets? | Pct% |
|---|---|
| Hacked systems and networks | 33% |
| Malicious code | 23% |
| Insider (spy/social engineer) | 20% |
| Intercepted voice communication | 10% |
| Paper documents | 9% |
| Other (please specify) | 5% |
| Total | 100% |

According to Table 4, one-third of respondents believe hacked systems and networks is the most likely venue by which unauthorized parities obtain valuable corporate secrets – followed by malicious code (which includes viruses, malware and botnets).

While not shown in the above chart, we asked respondents "What is the likelihood that your organization would not discover the wrongful interception of a cell phone conversation that revealed valuable corporate secrets?" About 80 percent of respondents state that it is not likely to be discovered, while only 7 percent state this it is very likely to be discovered within their organization today.

**2. IT practitioners are not confident that their organization's cell phones are secure.**

As reported in Pie Chart 3, only 33 percent say they are either very confident or confident that the proprietary and confidential information conveyed during cell phone conversations is adequately secured. Why are these respondents confident? According to Table 4, it is because of the belief that their organizations are unlikely to be targeted (76 percent), or that the cell phone has security features that prevent hacking and wrongful interception (61 percent). Another primary reason is the belief that corporate secrets are rarely discussed on cell phones (58 percent).

Pie Chart 1: How confident are you that the confidential information conveyed during cell phone conversations are secure?

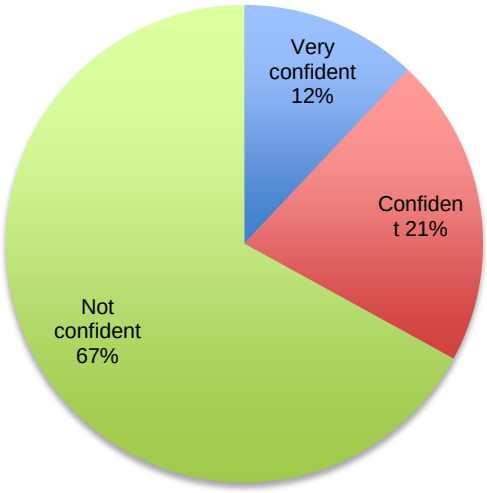


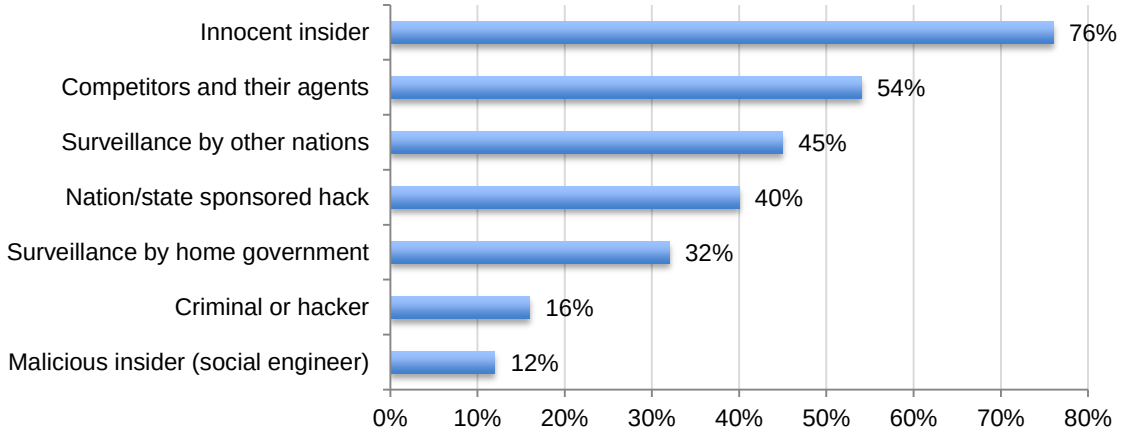

Table 5: Reasons why respondents feel confident or very confident. Please note that respondents could select more than one choice.

| If confident or very confident, why do you feel this way? | Pct% |
|---|---|
| Our organization is unlikely to be a target | 76% |
| Security technology on cell phones (such as encryption) prevents hacking | 61% |
| Corporate secrets are rarely discussed on phone conversations | 58% |
| Telephone service provider adequately secures communications | 45% |
| Employee compliance to policies is okay | 26% |
| Other reasons | 11% |

**3. Criminals and hackers are not considered the largest threat by most of the respondents.**

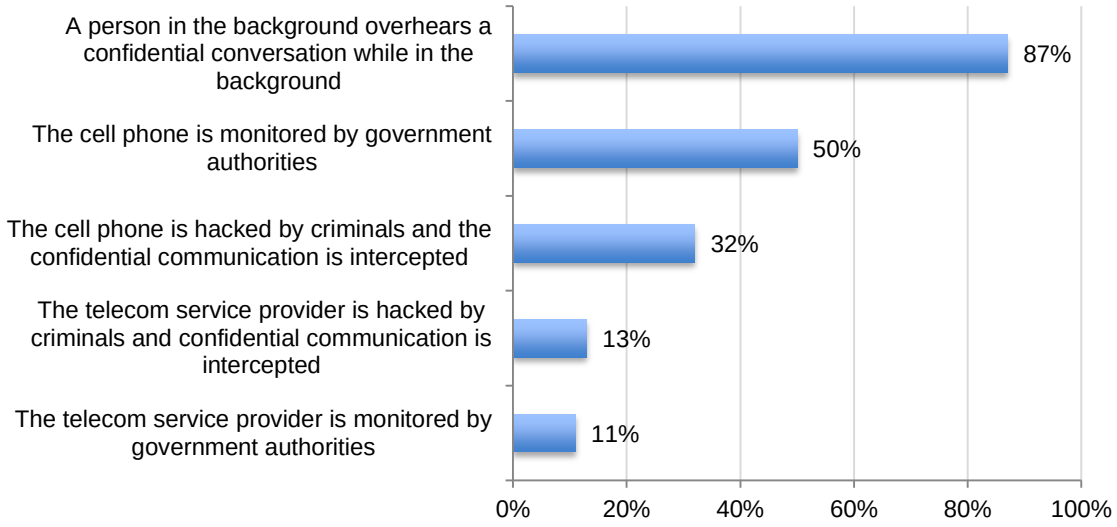
As shown in Bar Chart 2, the most likely person to acquire confidential information is the innocent insider (76 percent), followed by competitors and their agents (54 percent) and surveillance by other (foreign) nations (45 percent).

Bar Chart 2: The parties most likely to acquire confidential information or corporate secrets because of insecure phone communications



Bar Chart 3 shows 87 percent of respondents believe eavesdropping is a likely way corporate secrets are divulged from cell phone conversations with 50 percent indicating it is the result of monitoring by government authorities and 32 percent say it is due to criminals or hackers acquiring confidential information because of insecure cell phone communications.

Bar Chart 3: How corporate secrets are divulged from insecure cell phone communications




**4. Sales information and research and development information is most at risk as a result of insecure cell phone communications.**

Table 6 reports the forced rank and rank order of 10 information types potentially at risk because of insecure cell phone communications. Sales information is considered most at risk, followed by research and development, other trade secrets, and market strategies. Accounting and finance information and employee information appear to be less at risk according to respondents.

| Table 6. Ranking of the types of corporate secrets at risk because of insecure cell phone communications, where 1 = most at risk to 10 = least at risk. | Forced rank | Rank order |
|---|---|---|
| Sales information | 2.16 | 1 |
| Marketing and public relations information | 5.95 | 8 |
| Market strategies and plans | 3.84 | 4 |
| Research and development information | 2.92 | 2 |
| Business partnerships and joint ventures | 4.49 | 5 |
| Accounting and finance information | 7.65 | 9 |
| Customer information | 5.63 | 6 |
| Employee information | 8.00 | 10 |
| Legal and compliance information | 5.85 | 7 |
| Other trade secrets | 3.67 | 3 |
| Average | 5.02 | |

**5. The most risky regions for the interception of cell phone communications are Asia-Pacific and the Middle East.**

As shown in Table 7, North America and Europe are considered the least risky regions. Table 8 shows that the countries posing the greatest risk are China (PRC), the Russian Federation and the UAE. While participants identified these regions to pose the greatest risk to the security of

voice data, 70 percent say their organization is not using technologies such as encryption to secure cell phone communications and 83 percent are not training employees to be aware of the risk.

| Table 7: What regions of the world pose the **greatest risk** of intercepted voice data? Please select only three choices. | Pct% |
|---|---|
| Asia-Pacific | 95% |
| Middle East | 67% |
| Europe | 43% |
| Africa | 42% |
| North America | 35% |
| Latin America | 28% |

| Table 8: What countries pose the **greatest risk** of intercepted voice data? Top five countries. | Pct% |
|---|---|
| China (PRC) | 94% |
| Russian Federation | 80% |
| United Arab Emirates (UAE) | 76% |
| Saudi Arabia | 74% |
| Korea | 72% |
| Egypt | 72% |

**6. Very few organizations have a strategy for securing voice data across the enterprise.**

As shown in Pie Chart 2, 85 percent say that voice data security is equally important or more important than other security issues. Twelve percent see voice data security as less important. However, Table 9 reveals that 61 percent of respondents say their organizations do not have a plan to secure voice data across the enterprise. Only 9 percent of respondents say their organizations presently have an overall plan or strategy applied consistently.

Pie Chart 2: How important is voice data security relative to other security issues in your organization?

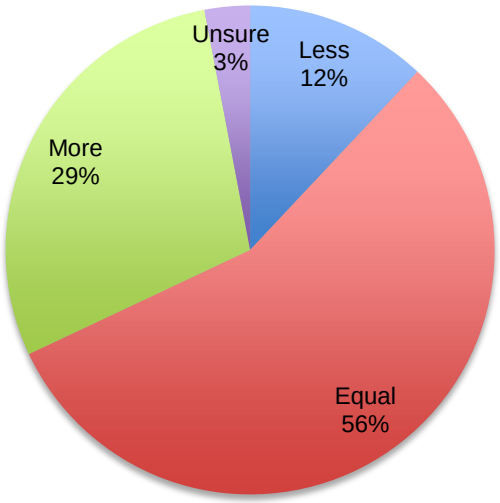
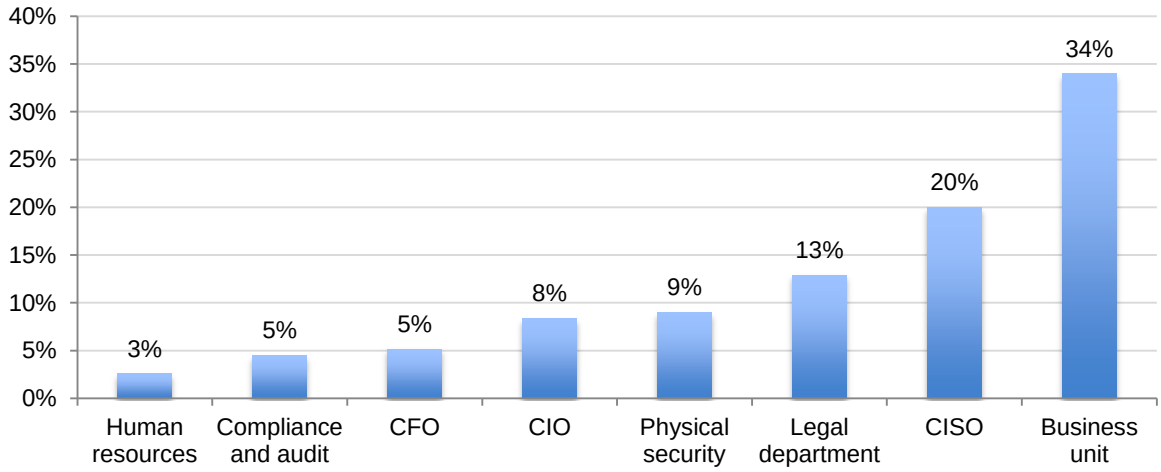



Table 9: One approach that best describes how organizations attempt to secure voice data across the enterprise.

| Approach to securing voice data across the enterprise. | Pct% |
|---|---|
| Formal enterprise strategy | 9% |
| Plan adjusted to situations | 12% |
| Informal plan | 18% |
| No plan or strategy | 61% |
| Total | 100% |

Bar Chart 4 reports that the business unit itself is considered by respondents to be most responsible for securing cell phone communication (34 percent), followed by information security (20 percent) and the legal department (13 percent). Only 5 percent of respondents see corporate IT as having primary responsibility for securing cell phone communications across the enterprise. A perceived low level of responsibility or involvement by the organization's CISO suggests voice data security is not handled as a normal or recurring information security threat within respondents' organizations.

Bar Chart 4: Who is most responsible for ensuring that confidential voice data is protected?

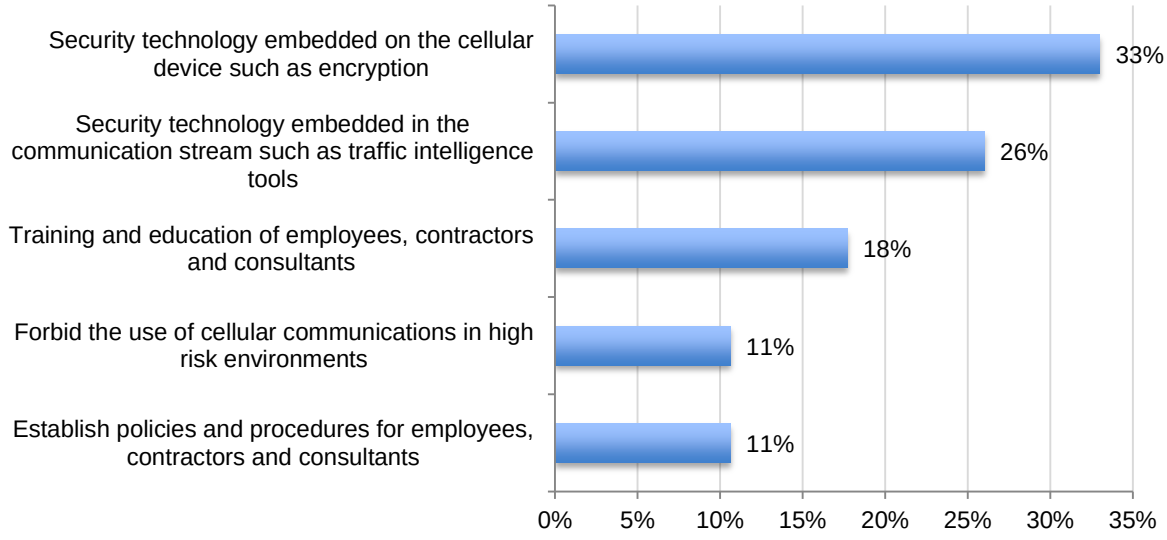



While not shown in the above chart, the primary activities for securing voice data today are forbidding the use of cell phones in high-risk areas (19 percent) and providing what are believed to be secure cellular phones (18 percent).

**7. Most IT practitioners seem to be uncertain as to the best way to reduce leakage of voice data.**

As shown in Bar Chart 5, 33 percent of respondents favor security technologies embedded on the cellular device such as encryption and 26 percent say the best way is to have security technologies embedded in the communication stream such as traffic intelligence tools. A smaller percentage of respondents believe training and polices and procedures are the best measures (18 percent and 11 percent, respectively). It is interesting that only 11 percent say the best way to reduce the leakage of cellular communications is to forbid the use of cellular communications in high-risk environments but, as noted above, it is a primary activity used to prevent leakage of voice data.

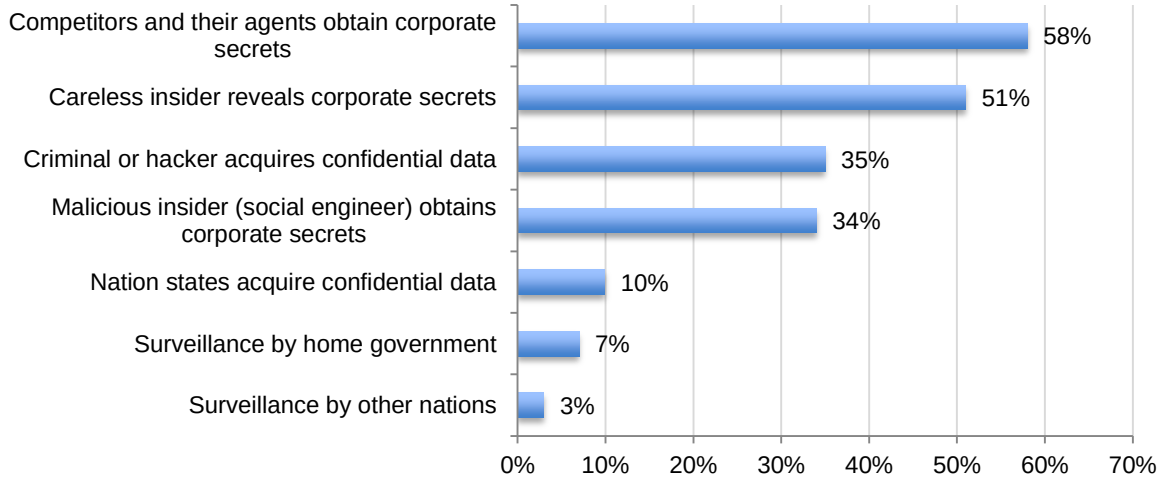
Bar Chart 5: The best ways to reduce the leakage of voice data in the workplace



**8. The most likely event to cause an organization to spend more on protecting voice data is if corporate secrets ended up in the hands of competitors and agents.**

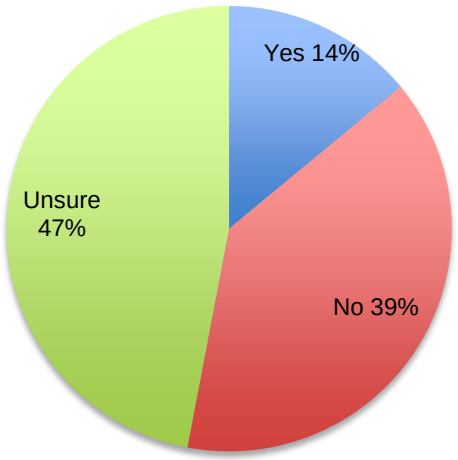
Bar Chart 6 reports seven triggering events that respondents believe will most likely motivate their organizations to focus on voice data security. The loss of corporate secrets to a competitor is viewed as the most significant trigger (58 percent). This is followed by careless or negligent employees revealing corporate secrets to outside parties (51 percent). Only 10 percent say that data acquisition by a foreign nation would trigger more spending or budget dollars.

Bar Chart 6: Triggering events most likely to cause expansion of effort and resources.

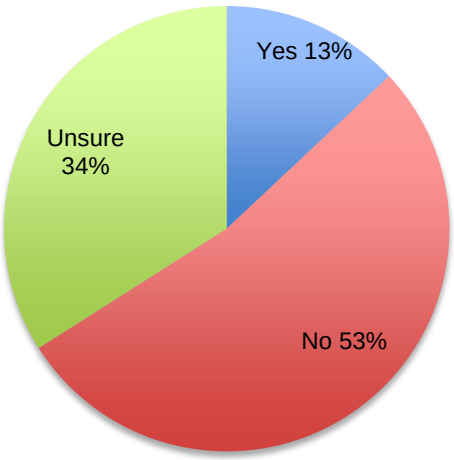



Pie Chart 3 shows respondents say that their organizations currently do not spend enough resources to prevent or reduce the risk of insecure voice data (39 percent) or are unsure (47 percent). According to Pie Chart 10, more than half of respondents (53 percent) report they do not have the right enabling technologies to prevent or reduce the risks caused by insecure voice data. Another 34 percent are unsure about the availability of security technologies.

Pie Chart 3: Does your organization spend enough resources to prevent or reduce the risk of insecure voice data?




Pie Chart 4: Does your organization have the right security technologies to prevent or reduce the risk of insecure voice data?



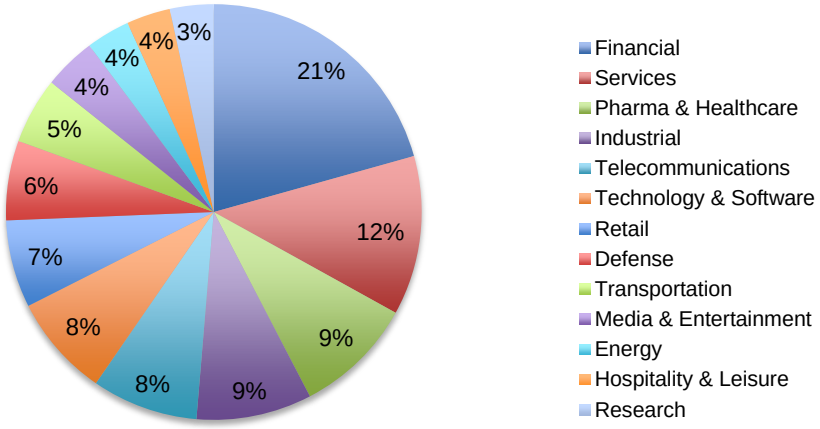
## III. Benchmark Methods

This study utilized a benchmark instrument to examine a panel of highly experienced IT and IT security practitioners and their views about voice data security in the context of their organization. In total, more than 650 individuals known to the researcher were personally contacted, resulting in 107 practitioners (representing 75 separate companies) agreeing to participate either by telephone or an in-person interview. All respondents are located in the United States.

Our interview method utilized a series of fixed formatted questions to ensure consistency and internal reliability. All questions included in the interview are included in Appendix 1 of this paper. On average, interviews were completed in less than one hour. In some cases the researcher was required to re-contact the respondent in order to clarify a specific response or obtain additional insights. All respondents were assured confidentially for themselves and their organizations.

The following pie chart shows the industry distribution of respondents' organizations. The largest industry segments are financial services (including banking, insurance, brokerage and credit cards), services (including professional services), and pharmaceuticals and healthcare.

Pie Chart 5: Industry distribution of respondents' organizations




The mean and median experience level of IT and IT security practitioners are 15.23 and 16.0 years, respectively. Table 10 provides the approximate job titles of respondents and Table 11 reports their organizational level.

| Table 10: Approximate title of respondents | Pct% |
|---|---|
| CISO | 21% |
| IT Security Director | 18% |
| CSO | 15% |
| IT Security Manager | 13% |
| IT Compliance | 13% |
| All other titles | 20% |
| Total | 100% |

| Table 11: Organizational level of respondents | Pct% |
|---|---|
| Senior Executive | 9% |
| Vice President | 18% |
| Director | 36% |
| Manager | 30% |
| Supervisor | 4% |
| Other (please specify) | 3% |
| Total | 100% |

Table 12 reports the worldwide headcount of respondents' organizations, showing that more than 45 percent of respondents working in larger-sized companies with more than 25,000 employees. Table 13 summarizes the respondents' roles in managing data protection and security risk. As can be seen, respondents self-report having a high level of involvement in setting priorities,

managing budgets, selecting vendors, determining data protection strategy, and evaluating program performance.

| Table 12: Worldwide headcount of respondents' organization | Pct% |
|---|---|
| Less than 500 | 8% |
| 500 to 1,000 | 11% |
| 1,001 to 5,000 | 15% |
| 5,001 to 25,000 | 31% |
| 25,001 to 75,000 | 23% |
| More than 75,000 | 12% |

| Table 13: Respondents' roles in managing data protection and security risk in your organization | Pct% |
|---|---|
| Setting priorities | 64% |
| Managing budgets | 60% |
| Selecting vendors | 71% |
| Determining strategy | 56% |
| Evaluating program performance | 59% |

**IV. Caveats**

Our benchmark study utilizes a diagnostic interview method that has been successfully deployed in earlier research. However, there are inherent limitations to benchmark research that need to be carefully considered before drawing conclusions from these findings.

- Non-statistical sample: The purpose of this study is descriptive inquiry rather than normative inference. This research draws upon a representative, but non-statistical sample of highly experienced IT and IT security practitioners.

- Non-response: The current findings are based on a small representative sample of companies. An initial invitation was sent to targeted individuals in more than 650 organizations. One hundred and seven individuals from 75 companies agreed to participate. Non-response bias was not tested so it is always possible companies that did not participate are substantially different on key aspects of voice data security.

- Sampling-frame bias: Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature data protection and information security programs.

- Unmeasured factors: To keep the survey concise and focused, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be estimated at this time.

## V. Implications for Organizations

The findings of this study highlight the need for organizations to take immediate steps to prevent the loss of proprietary and confidential information during cell phone conversations. However, as noted above, very few organizations are educating their employees about the risks. Here are some basic precautions that can be shared with employees.

- Never assume that voice calls are confidential (like fax or email), especially when calling internationally where some countries' phone operators have no encryption security in place at all. Check your signal, calls on 3G are more secure than 2G but often falls back to 2G when 3G is unavailable.

- Keep your phone safe and do not leave it lying around. Skilled attackers can take just a few moments to install a malicious program, compromise the security of the SIM card or install a special battery with a bug in it, all of which can later be used to help intercept calls.

- Use and protect your phone and voicemail PINs in the same way as your bankcard PIN. Never leave confidential messages in voicemails or send confidential texts. Texts in particular are easy to read on the phone and cell phone voicemails can often be accessed from any phone with the PIN.

- Be vigilant to prevent malicious software on your phone. Be wary of texts, system messages or events on your phone that you did not ask for, initiate or expect. Turn off Bluetooth if you are not using it. Consider anti-virus / anti-malware software, and if you strongly suspect your calls are being listened to then turn off the phone when you don't need it and remove the battery as an extreme precaution.

- Use voice call encryption software that works worldwide on your phone to secure your sensitive calls.

- If you have no alternative (such as using encryption software) and urgently need to discuss confidential matters over a cell phone:

    - Cover your mouth so you can't be lip-read
    - Choose a location where you can't be overheard
    - Talk quietly and be brief
    - Use code words
    - Split information across different channels (e.g. refer to emails or send texts etc so information is incomplete and meaningless on its own)

In summary, this report highlights the need to implement a strategy involving both technology and education for securing voice data. Like all security issues, it's important to balance the risk of loss against the convenience of communication. Users should be particularly aware of the risks when traveling to high-risk countries, discussing business-sensitive information or participating in conference calls where confidential information will be covered.

Organizations have a duty of care both to shareholders (to protect valuable information) and to individuals / employees (to protect privacy and personal security). Cell phone conversations, in addition to more traditional means such as email, must now be included in risk management policies and training and awareness programs. These findings should raise particular concern for those in highly regulated sectors, suggesting that voice communications now needs to be considered alongside other forms of data.

**For more information, please contact Ponemon Institute by email research@ponemon.org or visit our website at www.ponemon.org.**

**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 organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

## Appendix 1: Survey Details

The following tables summarize the results of our diagnostic interviews over a three-month period completed on February 24, 2010.

| Sample response | Freq. |
|---|---|
| Contacts made | 651 |
| Diagnostic interviews completed (judgmental sample) | 107 |
| Separate companies participating | 75 |

| **Part I. Attribution.** Please rate each one of the following seven statements using the scale provided below each item (only showing the strongly agree & agree combined response from a five point adjective scale). | Ex ante | Ex post |
|---|---|---|
| Q1a. In my organization, those who use cell phones understand the importance of not revealing confidential information during phone conversations (strongly agree & agree). | 52% | 41% |
| Q1b. In my organization, those who use cell phones understand the importance of not revealing confidential information when on business travel or in public places (strongly agree & agree). | 57% | 42% |
| Q1c. My organization has policies that strictly forbid the use of cell phones when discussing confidential information (strongly agree & agree). | 28% | 19% |
| Q1d. In my organization, it is unlikely that voice data communicated over a cell phone will be intercepted (strongly agree & agree). | 59% | 41% |
| Q1e. I don't worry about voice data because cell phones have security features that protect it (strongly agree & agree). | 49% | 29% |
| Q1f. Our telephone service provider has security that protects voice data (strongly agree & agree). | 48% | 33% |
| Q1g. I don't believe that criminals or spies target cell phone communications (strongly agree & agree). | 46% | 35% |

**Part II. Scenarios**

| **Conference Call**: An executive relies on his cell phone to participate in conference calls with other senior leaders in the company. During these calls, proprietary and confidential information about the company is sometimes exchanged. | Pct% |
|---|---|
| Q2a. How likely is it that this type of situation may occur in your organization (very likely & likely)? | 71% |
| Q2b. How prevalent is this practice among employees in your organization (very frequently)? | 76% |
| Q2c. Does your organization have a policy that forbids this practice (yes response)? | 19% |

| **Business travel**: A sales manager who travels extensively to China and other Asian countries uses her cell phone to communicate with the home office in the United States to coordinate sales strategy, pricing and contract information. During these calls, proprietary and confidential information is exchanged. | Pct% |
|---|---|
| Q3a. How likely is it that this type of situation may occur in your organization (very likely & likely)? | 80% |
| Q3b. How prevalent is this practice among employees in your organization (very frequently)? | 65% |
| Q3c. Does your organization have a policy that forbids this practice (yes response)? | 18% |

| **Third parties**: An outside lawyer contacts his client and requests proprietary and confidential information while using his cell phone. This requested information is provided by an employee over the phone. | Pct% |
|---|---|
| Q4a. How likely is it that this type of situation may occur in your organization (very likely & likely)? | 83% |
| Q4b. How prevalent is this practice among employees in your organization (very frequently)? | 68% |
| Q4c. Does your organization have a policy that forbids this practice (yes response)? | 21% |

| **Call center**: A customer contacts a company's call center to establish a new account. The information required from the customer includes her name, address, Social Security Number and other personal facts. This confidential information is conveyed to the call center over a cell phone. | Pct% |
|---|---|
| Q5a. How likely is it that this type of situation may occur in your organization (very likely & likely)? | 58% |
| Q5b. How prevalent is this practice among customers who contact your organization (very frequently)? | 35% |
| Q5c. Does your organization have a policy that forbids this practice (yes response)? | 29% |

| **Financial facts**: A company's finance and accounting staff has a conference call discussing a preliminary press release about quarterly earnings. One of the participants of the call is on a cell phone. | Pct% |
|---|---|
| Q6a. How likely is it that this type of situation may occur in your organization (very likely & likely)? | 62% |
| Q6b. How prevalent is this practice among employees in your organization (very frequently)? | 40% |
| Q6c. Does your organization have a policy that forbids this practice (yes response)? | 35% |

| **Location data**: A company's chief executive travels to another country to hold merger negotiations with the CEO and board of a major competitor. His administrative assistant uses a cell phone to arrange the CEO's ground transportation, which reveals the identity of the acquisition target. | Pct% |
|---|---|
| Q7a. How likely is it that this type of situation may occur in your organization (very likely & likely)? | 65% |
| Q7b. How prevalent is this practice among employees in your organization (very frequently)? | 41% |
| Q7c. Does your organization have a policy that forbids this practice ( yes response)? | 17% |

**Part III. Survey Questions**

| Q8a. How confident are you that the proprietary and confidential information conveyed during cell phone conversations are adequately secured? | Pct% |
|---|---|
| Very confident | 12% |
| Confident | 21% |
| Not confident | 67% |
| Total | 100% |

| Q8b. If confident or very confident, why do you feel this way? Please select up to three choices. | Pct% |
|---|---|
| Security technology on cell phones (such as encryption) prevents hacking | 61% |
| Telephone service provider adequately secures communications | 45% |
| Employee compliance to policies is okay | 26% |
| Our organization is unlikely to be a target | 76% |
| Corporate secrets are rarely discussed on phone conversations | 58% |
| Other | 11% |
| Total | 277% |

| Q9. In your opinion, how are confidential information or corporate secrets **most likely** to be divulged from cell phone communications? Please select up to three choices. | Pct% |
|---|---|
| A person in the background overhears a confidential conversation while in the background | 87% |
| The cell phone is hacked by criminals and the confidential communication is intercepted | 32% |
| The cell phone is monitored by government authorities | 50% |
| The telecom service provider is hacked by criminals and confidential communication is intercepted | 13% |
| The telecom service provider is monitored by government authorities | 11% |
| Other | 13% |
| Total | 206% |

| Q10. In your opinion, who is **most likely** to acquire confidential information or corporate secrets because of insecure cell phone communications within your organization? Please select up to three choices. | Pct% |
|---|---|
| Innocent insider | 76% |
| Malicious insider (social engineer) | 12% |
| Competitors and their agents | 54% |
| Criminal or hacker | 16% |
| Nation/state sponsored hack | 40% |
| Surveillance by home government | 32% |
| Surveillance by other nations | 45% |
| Other | 10% |
| Total | 285% |

| Q11. Do you believe that certain people (a.k.a. high risk employees such as executives, researchers, design engineers, and others) are targeted? For example, while on business travel or attending a conference event confidential communications of high-risk employees are targeted and intercepted. | Pct% |
|---|---|
| Absolutely certain | 15% |
| Yes, very likely | 31% |
| Yes, likely | 13% |
| No | 19% |
| Unsure | 22% |
| Total | 100% |

| Q12. In your opinion, who is most likely to divulge confidential information or corporate secrets while using a cell phone? | Pct% |
|---|---|
| Contractors, consultants and temporary employees | 27% |
| Staff level employees | 11% |
| Supervisors and managers | 12% |
| Directors and senior level managers | 27% |
| Top executives | 23% |
| Total | 100% |

| Q13. What types of corporate secrets are at risk because of insecure cell phone communications? Please rank order the following 10 information categories from 1 = most at risk to 10 = least at risk with respect to insecure cell phone communications. | Forced rank | Rank order |
|---|---|---|
| Sales information | 2.16 | 1 |
| Marketing and public relations information | 5.95 | 8 |
| Market strategies and plans | 3.84 | 4 |
| Research and development information | 2.92 | 2 |
| Business partnerships and joint ventures | 4.49 | 5 |
| Accounting and finance information | 7.65 | 9 |
| Customer information | 5.63 | 6 |
| Employee information | 8.00 | 10 |
| Legal and compliance information | 5.85 | 7 |
| Other trade secrets | 3.67 | 3 |
| Average | 5.02 | |

| Q14a. In your opinion, what regions of the world pose the **greatest risk** of intercepted voice data? Please select only three choices. | Pct% |
|---|---|
| North America | 35% |
| Europe | 43% |
| Africa | 42% |
| Latin America | 28% |
| Middle East | 67% |
| Asia-Pacific | 95% |
| Total | 310% |

| Q14b. In your opinion, what countries pose the **greatest risk** of intercepted voice data? Please select no more than five countries. | Pct% |
|---|---|
| China (PRC) | 94% |
| Russian Federation | 80% |
| Dubai | 76% |
| Saudi Arabia | 74% |
| Korea | 72% |
| Egypt | 72% |
| Average | 78% |

| Q15. Does your organization deploy technologies such as encryption to secure cell phone communications of employees who travel to high-risk locations? | Pct% |
|---|---|
| Yes | 14% |
| No | 70% |
| Unsure | 16% |
| Total | 100% |

| Q16. Does your organization conduct employee training to raise awareness about the insecure use of cell phones and the interception of voice data in high-risk locations? | Pct% |
|---|---|
| Yes | 10% |
| No | 83% |
| Unsure | 7% |
| Total | 100% |

| Q17. In your organization, who is **most responsible** for ensuring that confidential voice data is protected and secured? | Pct% |
|---|---|
| Business units (LOB) | 34% |
| CSO/CISO | 20% |
| Legal department (OGC) | 13% |
| Facilities management (physical security) | 9% |
| CIO (head of IT) | 8% |
| CFO | 5% |
| Compliance and audit | 5% |
| Other (please specify) | 3% |
| Human resources | 3% |
| Total | 100% |

| Q18. Please check one statement that **best describes** your organization's approach to securing voice data across the enterprise. | Pct% |
|---|---|
| We have an overall plan or strategy that is applied consistently across the entire enterprise. | 9% |
| We have an overall plan or strategy that is adjusted to fit different situations and businesses. | 12% |
| We have a limited or informal plan or strategy. | 18% |
| We don't have any plan or strategy. | 61% |
| Total | 100% |

| Q19. Please select all the activities that your organization presently does to securing voice data. | Pct% |
|---|---|
| Establishes policies | 15% |
| Forbids the use of cell phones in high risk locations | 19% |
| Trains employees and contractors about cell phone interception risk | 6% |
| Provides secure cellular phones | 18% |
| Monitors traffic to stop illegal interception | 8% |
| Deploys VOIP to replace conventional voice data communications | 13% |
| Other | 2% |
| None of the above | 20% |
| Total | 100% |

| Q20. In your opinion, how important is voice data security relative to other security issues that your organization deals with on a day-to-day basis? | Pct% |
|---|---|
| Less important | 12% |
| Equally important | 56% |
| More important | 29% |
| Can't determine | 3% |
| Total | 100% |

| Q21. In your opinion, what is the **best way** to reduce the leakage of voice data in the workplace? Please select only one choice. | Pct% |
|---|---|
| Establish policies and procedures for employees, contractors and consultants | 11% |
| Security technology embedded on the cellular device such as encryption | 33% |
| Security technology embedded in the communication stream such as traffic intelligence tools | 26% |
| Training and education of employees, contractors and consultants | 18% |
| Forbid the use of cellular communications in high risk environments | 11% |
| None of the above | 3% |
| Total | 100% |

| Q22. Please check one statement that **best describes** what you believe is the risk profile of voice data over the next 12 to 24 months. Please select only one choice. | Pct% |
|---|---|
| The risk of voice data losses resulting in the leakage of confidential information will increase. | 31% |
| The risk of voice data losses resulting in the leakage of confidential information will stay the same. | 49% |
| The risk of voice data losses resulting in the leakage of confidential information will decrease. | 9% |
| Can't determine | 11% |
| Total | 100% |

| Q23. From a risk perspective, which scenario concerns you most? Please select only one choice. | Pct% |
|---|---|
| Government intercepts cellular phone conversation of employees | 23% |
| Criminals intercept cellular phone conversation of employees | 25% |
| Both scenarios are equally risky | 52% |
| Total | 100% |

| Q24. How would you define the **scope** of the problem associated with insecure voice data? Please select only one choice. | Pct% |
|---|---|
| It mainly concerns executives in my organization. | 29% |
| It mainly concerns individuals at or above the supervisory level. | 24% |
| It concerns everyone in my organization who communicates from a cell phone. | 38% |
| It concerns all stakeholders including consultants, contractors and temporary employees. | 9% |
| Total | 100% |

**Part IV. Economic impact**

| Q25. In your opinion (best guess), what are the likely cost areas that are incurred as a result of voice data loss in your organization. Please allocate a total of 100 percentage points for the cost areas provided. | Percentage Points |
|---|---|
| Diminished value of intellectual properties | 36% |
| Lost revenues | 23% |
| Marketplace brand and reputation diminishment | 16% |
| Decreased productivity | 14% |
| Increased expenses | 8% |
| Customer loss or turnover | 2% |
| Other (please specify) | 1% |
| Total points | 100% |

| Q26. In your opinion (best guess), how much does it cost your organization **every time** a corporate secret is revealed to unauthorized parties, especially competitors and their agents? | Percentage Points | Extrapolated value |
|---|---|---|
| None | 0% | $- |
| Less than $10,000 | 4% | $320 |
| Between 10 and $100k | 6% | $3,000 |
| Between 101k and 500k | 19% | $47,500 |
| Between 501k and $1 million | 18% | $135,000 |
| Between 1 and $2 million | 26% | $390,000 |
| Between 2 and $4 million | 11% | $330,000 |
| More than $4 million | 10% | $440,000 |
| Don't know | 6% | $- |
| Total | 100% | $1,345,820 |

| Q27. In your opinion (best guess), how frequently is a corporate secret revealed to unauthorized parties each year, especially to competitors and their agents? | Pct% |
|---|---|
| Never | 5% |
| About once each year | 29% |
| About once every month | 43% |
| About once every week | 11% |
| About once every day | 7% |
| More than once every day | 0% |
| Don't know | 5% |
| Total | 100% |

| Q28. In your opinion (best guess), how do unauthorized individuals, especially competitors and their agents, obtain corporate secrets? Please allocate a total of 100 percentage points for the attack methods provided. | Percentage Points |
|---|---|
| Insider (spy/social engineer) | 20% |
| Paper documents | 9% |
| Intercepted phone communication | 10% |
| Hacked systems and networks | 33% |
| Malicious code, malware and botnets | 23% |
| Other (please specify) | 5% |
| Total points | 100% |

| Q29. In your opinion (best guess), what is the likelihood that you or your organization would **not discover** the wrongful interception of a cell phone conversation that revealed valuable corporate secrets? | Pct% |
|---|---|
| Not likely to be discovered | 80% |
| Likely to be discovered | 13% |
| Very likely to be discovered | 7% |
| Total | 100% |

| Q30. In your opinion, what triggering event is **most likely** to cause your organization to expend more effort to secure voice data? Please select no more than three choices. | Pct% |
|---|---|
| Careless insider reveals corporate secrets | 51% |
| Malicious insider (social engineer) obtains corporate secrets | 34% |
| Competitors and their agents obtain corporate secrets | 58% |
| Criminal or hacker acquires confidential data | 35% |
| Nation states acquire confidential data | 10% |
| Surveillance by home government | 7% |
| Surveillance by other nations | 3% |
| Other (please specify) | 0% |
| Total | 198% |

| Q31. Does your organization spend enough resources to prevent or reduce the risk of insecure voice data? | Pct% |
|---|---|
| Yes | 14% |
| No | 39% |
| Unsure | 47% |
| Total | 100% |

| Q32. Does your organization have the right security technologies to prevent or reduce the risk of insecure voice data? | Pct% |
|---|---|
| Yes | 13% |
| No | 53% |
| Unsure | 34% |
| Total | 100% |

**Part V. Organizational characteristics and respondent demographics**

| D1. Your current title is (please specify) | Pct% |
|---|---|
| CISO | 21% |
| IT Security Director | 18% |
| CSO | 15% |
| IT Security Manager | 13% |
| IT Compliance | 13% |
| All other titles | 20% |
| Total | 100% |

| D2. What organizational level best describes your current position? | Pct% |
|---|---|
| Senior Executive | 9% |
| Vice President | 18% |
| Director | 36% |
| Manager | 30% |
| Supervisor | 4% |
| Staff or technician | 0% |
| Other (please specify) | 3% |
| Total | 100% |

| D3. Check the **Primary Person** you or your supervisor reports to within your organization. | Pct% |
|---|---|
| CEO/Executive Committee | 10% |
| Chief Financial Officer | 9% |
| Chief Information Officer | 26% |
| Compliance Officer | 9% |
| Chief Privacy Officer | 0% |
| Director of Internal Audit | 2% |
| General Counsel | 5% |
| Chief Technology Officer | 9% |
| Human Resources VP | 2% |
| Chief Security Officer | 14% |
| Chief Risk Officer | 11% |
| Other (please specify) | 2% |
| Total | 100% |

| D4. Check the country or U.S. region where your company's **primary** headquarters is located. | Pct% |
|---|---|
| Northeast | 20% |
| Mid-Atlantic | 19% |
| Midwest | 18% |
| Southeast | 13% |
| Southwest | 12% |
| Pacific | 18% |
| Total | 100% |

| Experience (mean & median years) | Mean | Median |
|---|---|---|
| D5a. Total years of business experience | 15.23 | 16.00 |
| D5b. Total years in corporate IT or IT security | 13.49 | 14.00 |
| D5c. Total years in current position | 5.25 | 5.50 |

| D6. Educational and career background: | Pct% |
|---|---|
| Compliance (auditing, accountant, legal) | 12% |
| IT (systems, software, computer science) | 34% |
| Security (law enforcement, military, intelligence) | 28% |
| Other non-technical field | 11% |
| Other technical field | 15% |
| Total | 100% |

| D7. What industry best describes your organization's industry concentration or focus? | Pct% |
|---|---|
| Banking | 11% |
| Manufacturing | 9% |
| Professional Services | 8% |
| Technology & Software | 8% |
| Retail | 7% |
| Defense | 6% |
| Health Care | 5% |
| Pharmaceutical | 4% |
| Telecommunications | 4% |
| Media & Entertainment | 4% |
| Services | 4% |
| Cable | 3% |
| Credit Cards | 3% |
| Hospitality & Leisure | 3% |
| Insurance | 3% |
| Research | 3% |
| Energy | 3% |
| Transportation | 3% |
| Education | 3% |
| Automotive | 2% |
| Brokerage | 2% |
| Total | 100% |

| D8. What best describes your role in managing data protection and security risk in your organization? Check all that apply. | Pct% |
|---|---|
| Setting priorities | 64% |
| Managing budgets | 60% |
| Selecting vendors and contractors | 71% |
| Determining privacy and data protection strategy | 56% |
| Evaluating program performance | 59% |
| Total | 310% |

| D9. What is the worldwide headcount of your organization? | Pct% |
|---|---|
| Less than 500 people | 8% |
| 500 to 1,000 people | 11% |
| 1,001 to 5,000 people | 15% |
| 5,001 to 25,000 people | 31% |
| 25,001 to 75,000 people | 23% |
| More than 75,000 people | 12% |
| Total | 100% |