

Security of Voice Data

Executive Summary

Prepared by Larry Ponemon, March 2010

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 said 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.

Part I. Attributions

The study seeks to understand the level of awareness IT practitioners have about voice data security and how important they believe it is to secure cell phone communications. In this section of the survey, we asked respondents questions about whether they agree or disagree that their organizations' executives 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.

In this part of the study, we divided the sample into two parts. We asked one group to respond to attribution questions prior to the scenarios (described below) and the second group to respond at the conclusion of the survey. We learned that those who responded to attribution questions at the beginning of the survey (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 (ex post respondents) were more likely to believe that the risk is real and that cell phone communications are at risk. This suggests that the survey questions and scenarios informed participants and increased their awareness of the threats to voice data.

Part II. Scenarios

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. The scenarios described the following:

- A conference call among senior leaders in the company where cell phones are sometimes used;
- A sales manager conducting business in Asia uses her cell phone to communicate with the home office;
- An external lawyer asks for proprietary and confidential information while using his cell phone;
- A call center employee assists a customer using a cell phone to establish an account and collects personal information (including Social Security number);
- The finance and accounting staff discusses an earnings press release and one participant on the call is using a cell phone; and
- A CEO's administrative assistant uses a cell phone to arrange ground transportation which reveals the CEO's identity and location.

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).

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).

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.

Part III. Key Survey Findings

The interception of corporate secrets during cell phone conversations is costly and not likely to be discovered. The average cost to an organization every time a corporate secret is revealed to unauthorized parties, especially agents and their competitors, is \$1.3 million. Forty-three percent of respondents believe this occurs about once every month and 29 percent believe it happens annually. Thirty-three percent of respondents believe hacked systems and networks is the number one way unauthorized individuals obtain corporate secrets followed by malicious code, malware and botnets. Eighty percent believe that the organization would not discover the wrongful interception of a cell phone conversation that revealed valuable corporate secrets.

IT practitioners are not confident that their organization's cell phones are secure. Only 33 percent say they are very confident or confident that the proprietary and confidential information conveyed during cell phone conversations is adequately secured. If they are confident, it is because they believe their organization is unlikely to be a target (76 percent), cell phone security prevents hacking (61 percent) and corporate secrets are rarely discussed on cell phones (58 percent). Respondents could select more than one choice.

Criminals and hackers are not considered the largest threat by most of the respondents. Eighty-seven percent of IT practitioners surveyed 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 due to criminals or hackers acquiring confidential information because of insecure cell phone communications. The most likely person

to acquire confidential information is the innocent insider, according to 76 percent of respondents followed by competitors and their agents (54 percent).

Sales information and research and development information is most at risk. Other types of information at risk are legal and compliance information and market strategies and plans. Not likely to be at risk are accounting and finance information and employee information.

The most risky regions for the interception of voice data are Asia-Pacific and the Middle East. North America and Europe are considered the least risky regions. The countries that pose the greatest risk are China (PRC), the Russian Federation and Dubai. 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.

Very few organizations have a strategy for securing voice data across the enterprise. Although 86 percent say that voice data security is equally important or more important than other security issues, 61 percent say they don't have a plan to secure voice data across the enterprise. The group most responsible for securing cell phone communication seems to be the business units (34 percent of respondents) and not IT. The primary activities for securing voice data are forbidding the use of cell phones in high risk areas (19 percent) and providing secure cellular phones (18 percent).

IT practitioners seem to be uncertain as to the best way to reduce leakage of voice data. Thirty-three percent 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 policies 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.

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 (58 percent). This is followed by having a careless insider reveal corporate secrets (51 percent). Only 35 percent say that a criminal or hacker acquiring confidential data would trigger more spending.

IT practitioners say that their organization currently does not spend enough resources to prevent or reduce the risk of insecure voice data (39 percent) or are unsure (47 percent) More than half (53 percent) report they do not have the right technologies to reduce this risk and 34 percent are unsure.

IV. 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 sum, this report highlights the need 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.

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.