Global Visual Hacking Experimental Study: Analysis

Sponsored by 3M Company

Independently conducted by Ponemon Institute LLC

Publication Date: August 2016

Global Visual Hacking Experimental Study: Analysis

By Ponemon Institute, August 2016

Part 1. Introduction

Ponemon Institute is pleased to present the results of the *Global Visual Hacking Experimental Study: Analysis*, sponsored by 3M Company

This research extends earlier U.S. research[1] (published in February 2015) to organizations located in the following seven countries: China, France, Germany, India, Japan, South Korea and the United Kingdom. The purpose of this research is to test an organization's readiness to prevent and detect visual hacking in the business office environment. Visual hacking occurs when employees make poor choices in how they access and display sensitive information, which is then seen and read by either a curious individual or a malicious hacker. Sensitive information can be displayed on laptops, tablets and smartphones, as well as in paper documents that are left in plain sight on desks, printers and conference tables and at other office locations or outside meeting sites.

Findings reveal that many organizations need to create awareness among employees on the need to protect sensitive information in clear view of unauthorized parties including potential visual hackers.

The 2016 study at a glance

Visual hacking is a global problem. Visual hacking occurred in all countries and 91 percent of 157 visual hacking attempts (trials) were successful.

A company's most sensitive information is at risk. Twenty-seven percent of the data hacked is considered sensitive information.

Certain situations are more risky. Documents on vacant desks and data visible on computer screens are most likely to be hacked.

Visual hacking happens quickly. It took less than 15 minutes to complete the first visual hack in 49 percent of the hacking attempts.

Office workers are timid about confronting a visual hacker. In 68 percent of the hacking attempts, office personnel did not question or report the visual hacker even after witnessing unusual or suspicious behavior.

Office layout affects visual hacking. Traditional offices and cubicles make it easier to protect paper documents and more difficult to view a computer screen. In contrast, the open floor plan appears to exacerbate the risk of visual hacking.

How serious is the risk of visual hacking? Our study found 91 percent of visual hacking attempts were successful. Moreover, visual hacks happened very quickly; that is, it took the visual hacker less than 15 minutes to acquire sensitive or confidential information for 49 percent of experimental trials. The following are reasons why visual hacking is a serious risk for organizations:

- To increase productivity, many organizations are creating open workspaces without walls and cubicles. As a result, it is more likely that sensitive and confidential documents and unprotected computer screens will be visible to prying eyes.
- In general, organizations are better able to enforce access policies for electronic documents in a consistent fashion across all users than for paper documents.
- Employees or contractors often are not aware of what types of information are sensitive or confidential and should be protected from individuals with malicious intent.
- Many organizations do not have a visual privacy policy or awareness program for securing paper documents both within the office and at off-site locations.
- Employees often neglect to shred or dispose of sensitive paper documents in a secure manner. Confidential paper documents thrown in a trash bin, left in a communal printing tray and at an office desk are particularly vulnerable to visual hacking.
- Sensitive and confidential documents are frequently accessed in public locations because of the increasingly mobile workforce.
- Organizations do not require the use of privacy filters to block sensitive or confidential information on computer screens, tablets or smartphones from prying eyes.

Part 2. Experimental Methods

[1]See: *Visual Hacking Experimental Study*, conducted by Ponemon Institute and sponsored by 3M, February 2015.

Ponemon Institute conducted a "white hat" experiment involving actual visual hacking in real workplace settings located in eight countries. Our mission was to test organizations' readiness to detect and prevent visual hacking in the business office environment. Ponemon Institute's benchmark community members were contacted for participation in this research.[2]

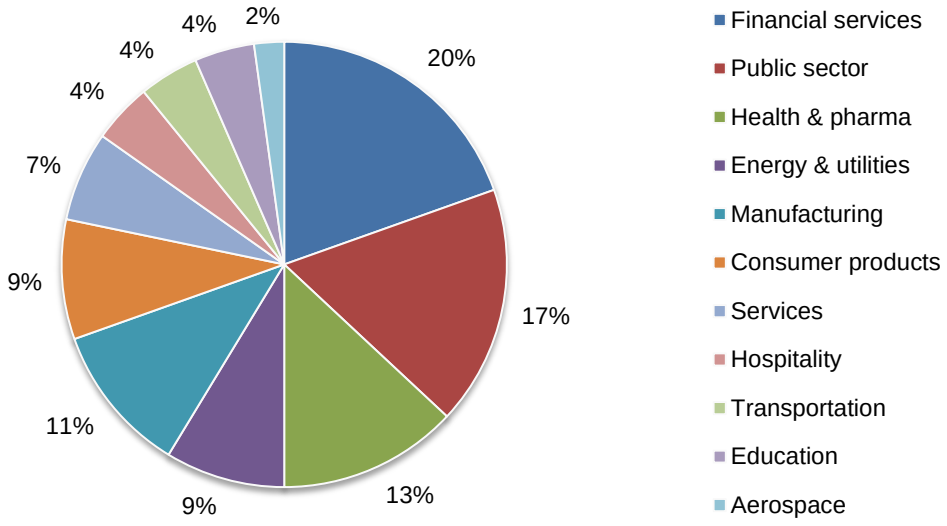
We recruited 46 companies that allowed us to field our experiment within actual office locations. As noted in Table 1, a total of 157 trials were conducted.[3] By design, all field experiments occurred on premises during the normal workday.[4]

Table 1: Frequencies of companies and trials

Country locations	Actual number of companies providing office venues	Completed trials
United States	8	43
United Kingdom	6	23
India	8	22
Korea	5	18
Germany	7	17
Japan	5	13
China	4	11
France	3	10
Totals	46	157

Figure 1 shows the primary industry classification of 46 participating companies. Eleven industries are represented in this study. The largest segments are financial services, public sector and health and pharmaceuticals.

Figure 1. Distribution of sponsoring companies by industry
n = 46 organizations; 8 countries (combined)



[2]This benchmark community consisted of 1,613 organizations at the time of this study.
[3]The earlier study's U.S. results are combined with the current results from seven additional countries. Forty-three trials for U.S. organizations were conducted in July 2014. The additional 114 trials were conducted in seven countries from mid-January through early April 2016.
[4]In most cases, participating companies used experimental results as part of training and awareness efforts.

Figure 2 shows 11 functional areas that provided the venues for this study. The largest functional areas were customer services and data center operations.

Figure 2. Distribution of experimental trials by office function
n = 157 trials; 8 countries (combined)

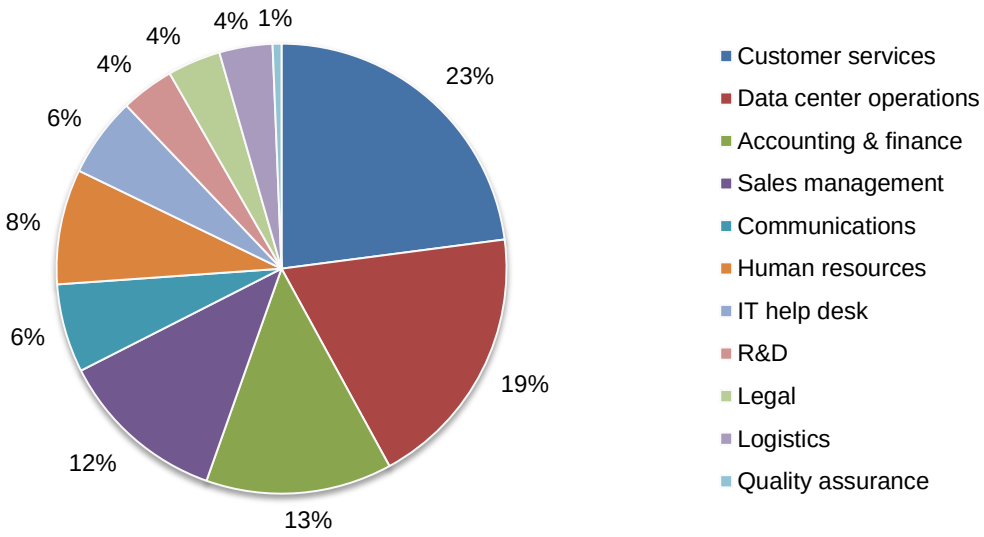
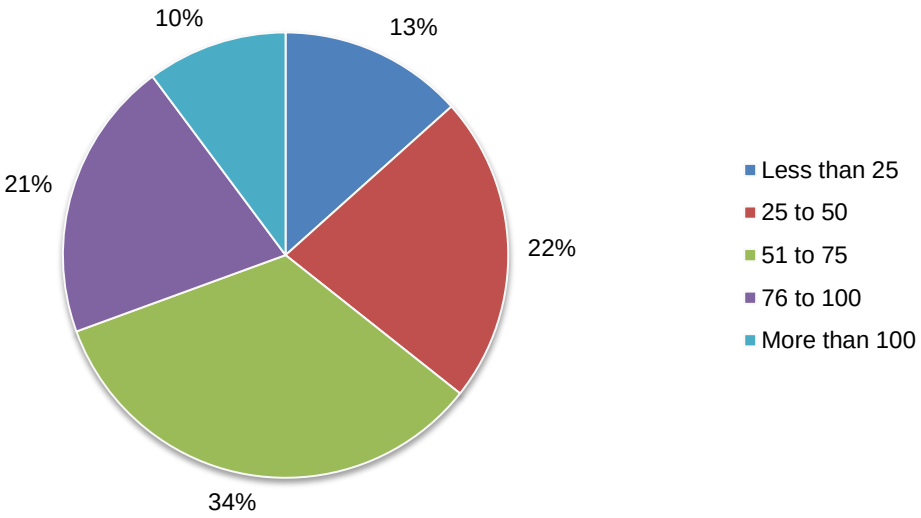


Figure 3 summarizes the headcount of employees who were located in the business office where the visual hacking experiment took place. Sixty-five percent of trials were conducted in local offices with 50 or more employees.

Figure 3. Distribution of experimental trials by office headcount
n = 157 trials; 8 countries (combined)



The researcher (a.k.a. visual hacker) was permitted to enter work areas and observe possible information leaks viewed from unprotected paper documents, computer screens (terminals, desktops and laptops) and other mobile devices. While the researcher was a passive observer, she or he was permitted to handle actual documents residing in open spaces on copiers, printers and fax machines. The researcher was not permitted to capture images by camera or scanning technologies.

With the aid of a company liaison, the researcher posed as a temporary office worker or consultant with a temporary identity credential to enter and exit normal spaces, including locations where electronic equipment resided.[5] With the exception of the company liaison, office workers in each location were not told in advance about the study and were only given minimal information about the role and function of the temporary worker or consultant.

The experiment required the researcher to record the type of potentially sensitive or confidential information observed during one two-hour session at each location. To preserve confidentiality, the actual information observed by the researcher was not revealed in the record inventory. Following are the different types of information that could be recorded by the researcher:[6]

- Personally identifiable information
- Information about customers or consumers
- Information about employees
- General business correspondence
- Access and login information/credentials
- Confidential or classified documents
- Attorney-client privileged documents
- Financial, accounting and budgeting information
- Design documents, presentations and architectural renderings
- Photos and videos containing business information
- Training materials

At the conclusion of each trial, the company's liaison introduced the researcher to office workers in the immediate office space where the experiment was conducted. These office workers were asked to complete a debriefing survey to assess their perceptions and level of awareness about the experiment.

About the experiment

This study involved one researcher assuming the role of a visual hacker. The researcher wore a temporary security badge. The researcher was also assigned desk space and provided Internet connectivity through the visitor's network. In most cases, the company liaison introduced the researcher as a temporary or part-time worker to office workers in adjacent or nearby desks. The researcher performed the following three tasks in full view of fellow office workers:

Task 1: The first task required a relatively inconspicuous office walk-through to scout for information in full view on desks, screens and other indiscrete locations. This office walk-through procedure required the researcher to maintain a log of information types directly observable.

Task 2: The second task required the researcher to grab a stack of business documents labeled as "confidential" off a nearby vacant table or desk and quickly put these documents in a briefcase. By design, this task was completed in full view of office workers.

Task 3: The third and final task was the most conspicuous to office workers. Here, the researcher used his or her smartphone's digital camera to take pictures of what appeared to be business confidential information on the computer screen or terminal.

Debrief: At the conclusion of all three tasks, the company liaison and researcher conducted a debriefing session with office workers located in the area of the experiment to determine their perceptions and level of awareness about visual hacking. Did these office workers recognize this as a suspicious event or incident? If so, what actions did they take or fail to take to stop it? In most cases, this debriefing session was conducted on the same day as the experiment.

[5]The company liaison was a supervisor or manager located in each office where the experiment was conducted. Approximately two weeks before the experiment, this individual was given explicit instruction by the researcher on the purpose of the research and the need for secrecy.
[6]The researcher was instructed not to perform extraordinary tasks to observe documents or displayed data. Hence, the researcher relied solely upon casual observation to record information types.

Part 3. Key Findings

Figure 4 provides the time distribution for the completion of 157 experimental trials. As can be seen, 38 (2+8+28) percent of trials (not including debriefing) were completed in less than two hours.

Figure 4. Histogram on the minutes to complete three experimental tasks
n = 157 trials; 8 countries (combined)

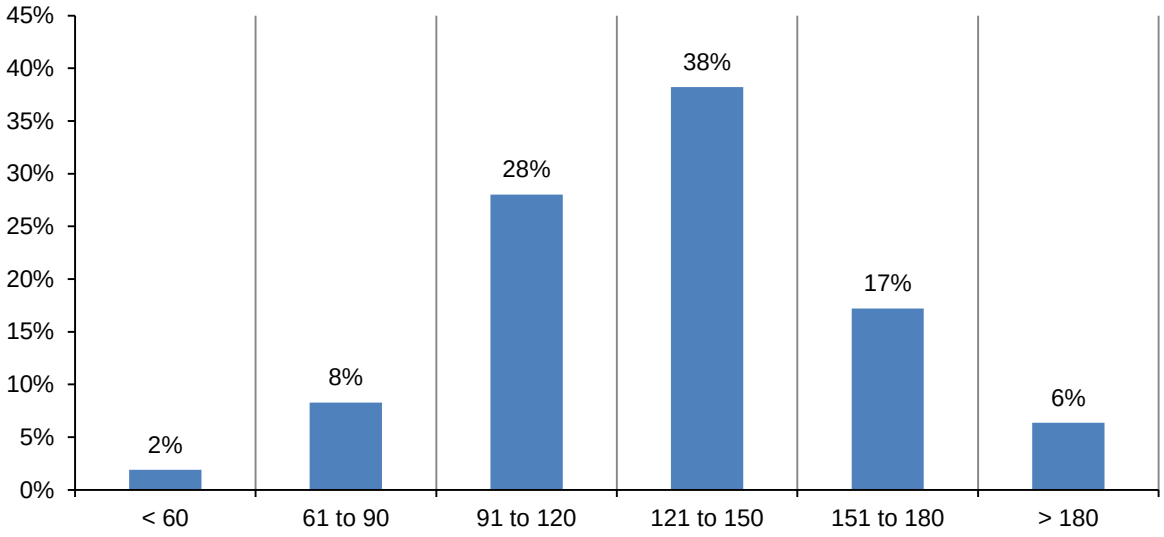
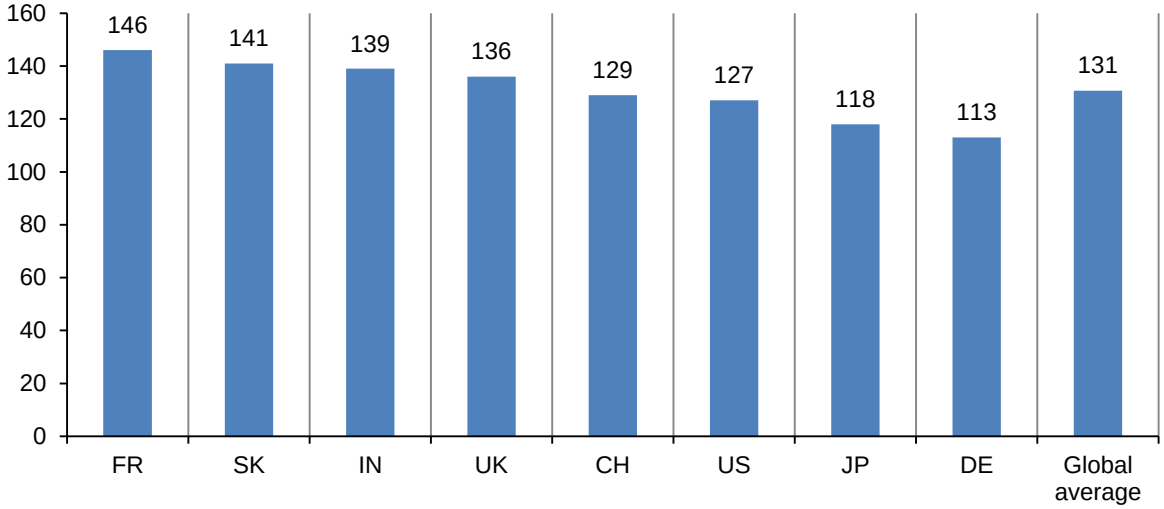


Figure 5 shows the average minutes to complete all tasks by country.[7] The average total time to complete all three experimental tasks was 131 minutes (not including the debriefing session). Trials conducted in Germany had the lowest time to complete all experimental tasks. In contrast, trials conducted in France and Korea had the highest time to complete.

Figure 5. Average minutes to complete three experimental tasks by country
Global average (baseline) = 131 minutes
n = 157 trials



[7] Following are the abbreviations used to identify country samples: CH=China, DE=Germany, FR=France, IN=India, JP=Japan, SK=Korea, UK=United Kingdom, and US=United States.

A total of 613 instances of visually hacked information occurred in 157 experimental trials (an average of 3.9 instances per trial).

Table 2: Frequency of breached data types for 157 experimental trials (613 pieces of data)

Information types	SK	US	UK	CH	JP	DE	FR	IN	Total
Access and login information/credentials	9	19	8	7	6	4	7	9	69
Attorney-client privileged documents	1	3	2	0	1	0	1	2	10
Confidential or classified documents	5	12	5	2	1	1	5	9	40
Contact list and directory	14	29	11	6	7	7	10	19	103
Design documents or architectural renderings	3	10	3	3	1	0	1	2	23
Financial, accounting and budgeting information	5	17	3	3	2	1	3	15	49
General business correspondence	2	16	7	2	1	5	4	11	48
Information about customers or consumers	20	21	7	12	4	6	8	23	101
Information about employees	11	16	12	8	6	3	5	14	75
Photos and videos containing business information	5	12	4	2	1	1	3	6	34
Presentations	3	9	3	2	2	3	2	3	27
Training materials	2	4	6	3	4	3	4	8	34
Total number of breached data types	80	168	71	50	36	34	53	121	613

Figure 6 provides the percentage frequency of information types visually hacked in this study. The information type most frequently hacked contained contact lists and directories (including employee directories). At two percent, attorney-client privileged information was the least likely to be visually hacked in this experiment.

Figure 6. Percentage frequency of information types visually hacked
n = 613 pieces of data; 8 countries (combined)

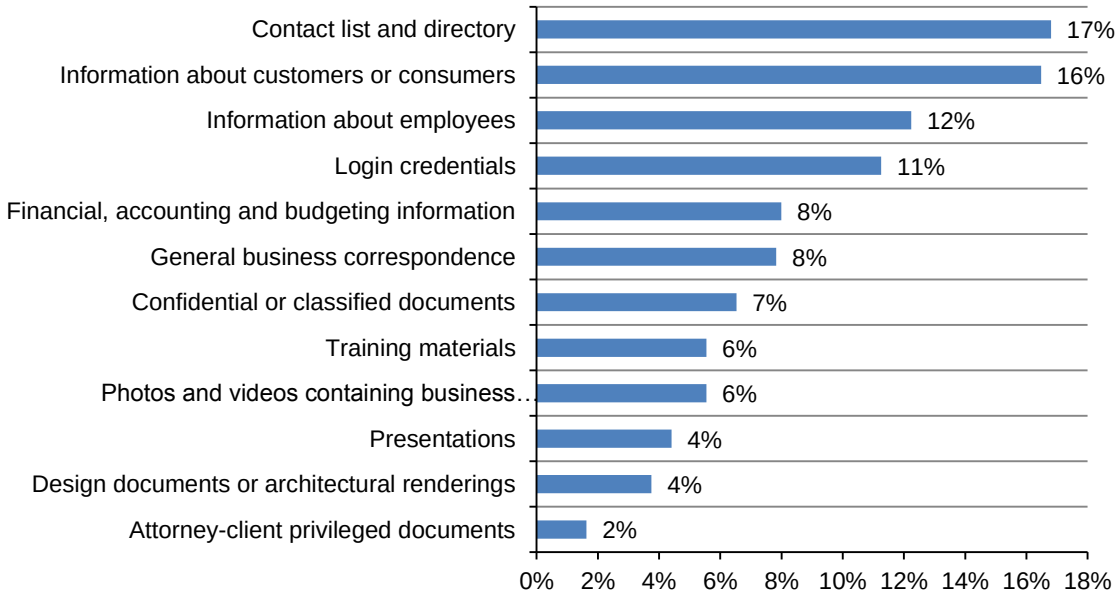
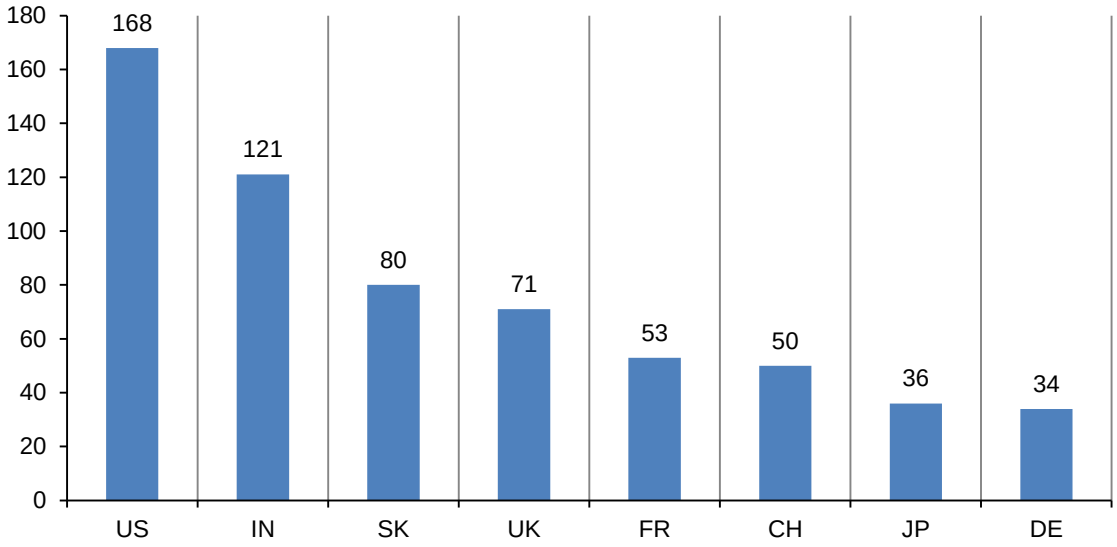


Figure 7 summarizes the distribution of 613 visual privacy breaches for the eight-country sample. For 43 trials conducted in the U.S., the visual hacker was able to view 168 separate pieces of data (i.e., visual privacy breaches). Similarly, for 10 trials conducted in Germany, the visual hacker was able to view 34 pieces of data.

Figure 7. Frequency of breached data types, by country (not weighted)
n = 613 pieces of data



As can be seen in Figure 8, the average number of visually breached data types varies considerably, from a low of 2.0 in Germany to a high of 5.5 in India. The global average was 3.9.

Figure 8. Average number of visually breached data types, by country
Global average (baseline) = 3.9 breached data types
Weighted by the number of trials

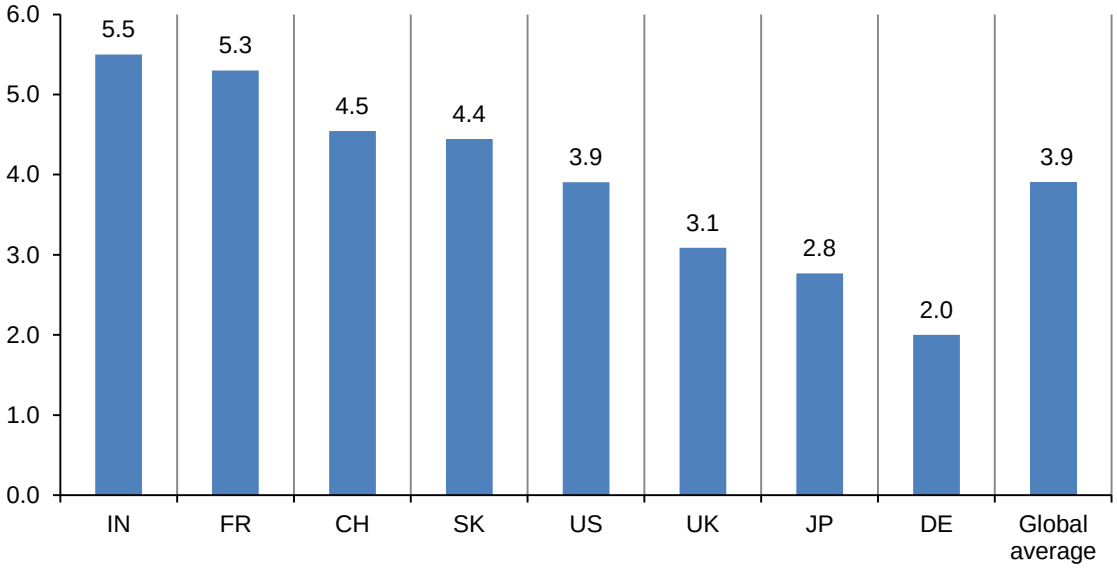


Figure 9 reports the frequency distribution for the number of breached data types observed by the visual hacker for all 157 experimental trials. As reported, 14 trials (or 9 percent) did not experience a visual hack.[8] In other words, 91 percent of experimental trials experienced at least one instance of visual hacking. A total of 18 of 157 trials experienced more than six information types observed by the researcher.

Figure 9. Histogram of information types captured
n = 157; 8 countries (combined)

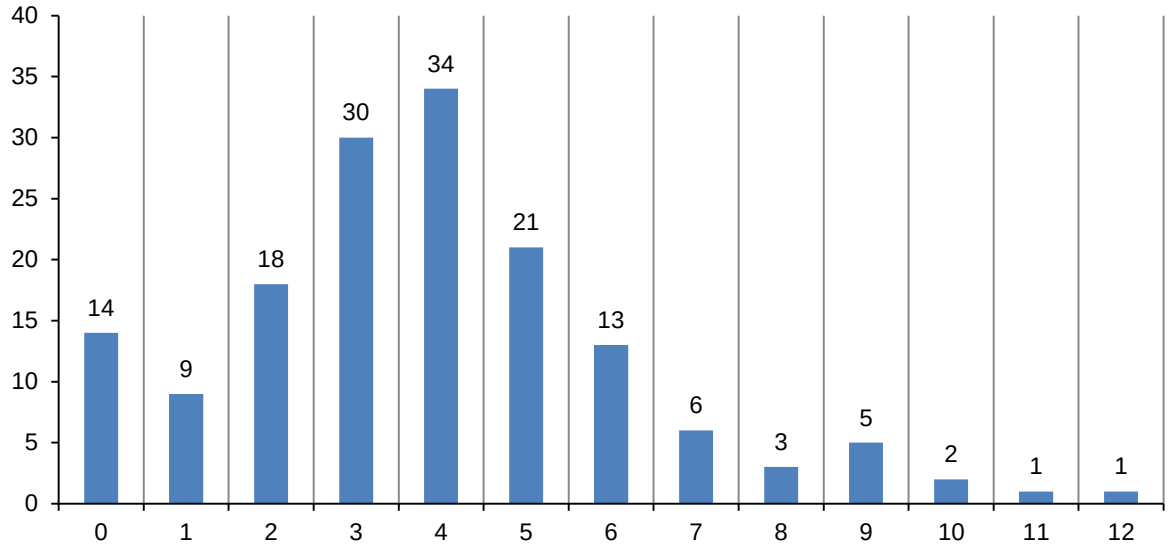
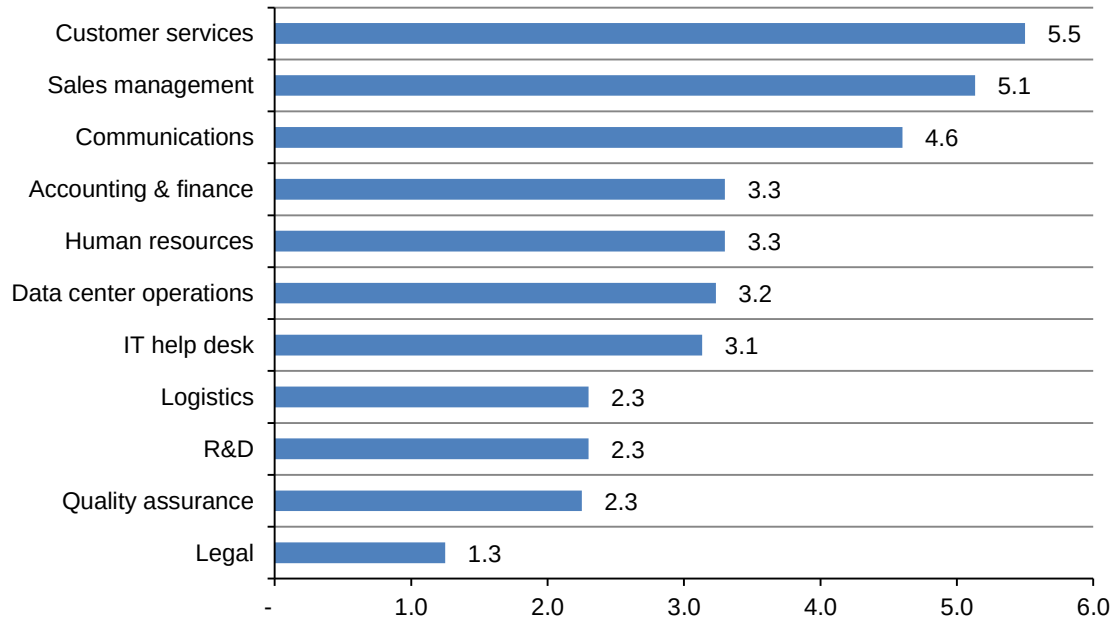


Figure 10 shows significant variation among functional areas. Experimental trials conducted in customer services had the most information types visually hacked. In contrast, legal had the least number of information types visually hacked.

Figure 10. Average number of information types visually hacked by functional area
n = 157 trials; 8 countries (combined)



[8]Of the five experimental trials that did not experience any visual hack, three involved office locations of one defense and aerospace company. The remaining two involved an education/research organization.

The next chart shows the average number of visual data breaches by the approximate headcount of participating business offices. As noted in Figure 11, smaller-sized offices with 25 to 50 employees had the lowest number of visually hacked data types (at 3.4). Offices with 76 to 100 employees had the highest number of hacks (at 4.6).

Figure 11. Average number of visually breached data types by office headcount
n = 157 trials; 8 countries (combined)

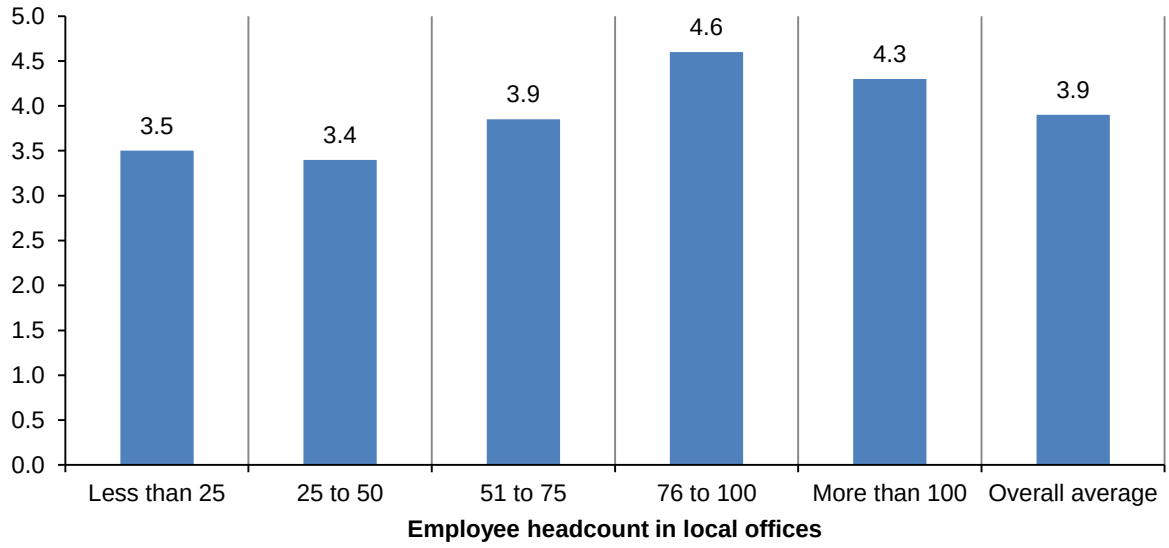
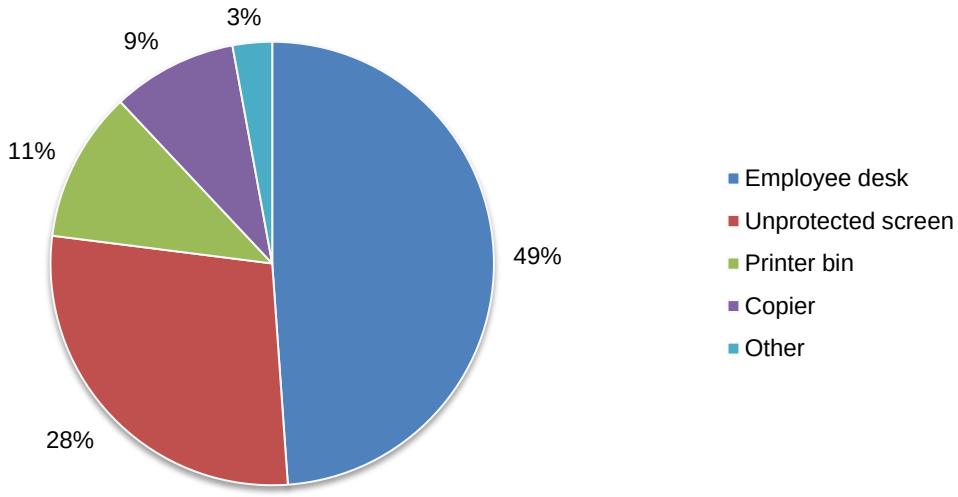


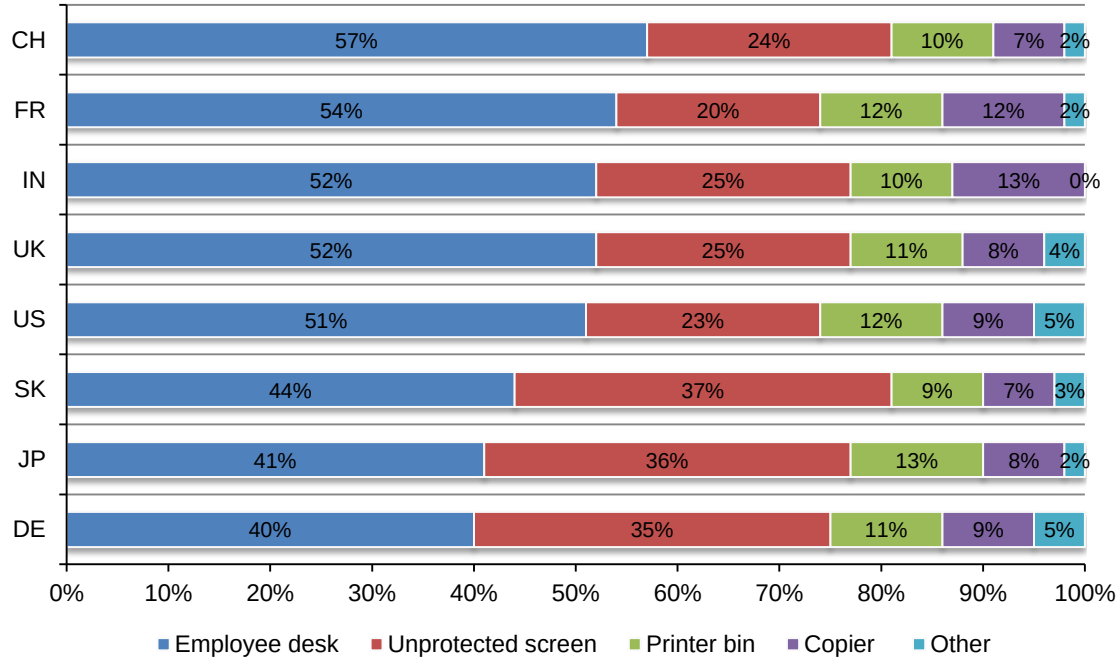
Figure 12 summarizes the location where sensitive or confidential information was observed by the researcher. As shown, 49 percent of all visual hacks involved documents visible on employees' desks. Another 28 percent of visual hacks involved information gleaned from unprotected desktops, laptops, tablets and other mobile devices.

Figure 12. Where the visual hacking occurred for all information types
n = 613 pieces of data; 8 countries (combined)



The following figure shows the location of the visual hack by country. At 57 percent, China had the highest-percentage frequency for employee desk. At 37 percent, Korea had the highest-percentage frequency for unprotected computer screen.

Figure 13. Where visual hacking took place by country
n = 613 pieces of data



Of all 613 pieces of visually breached data, 168 pieces (27 percent) were designated sensitive information assets. In short, this information was deemed to be sensitive because of the potential security risk to the organization in the aftermath of a data breach incident.

Figure 14. Proportion of high sensitive information
n = 613 pieces of data; 8 countries (combined)

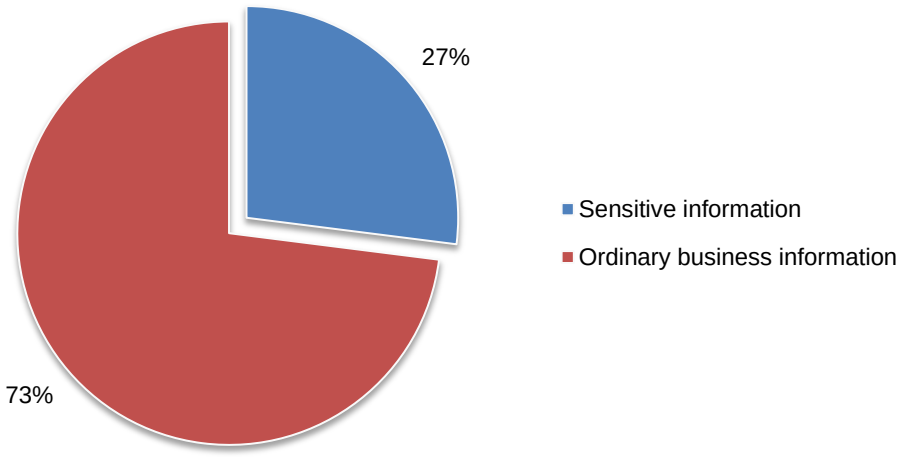


Figure 15 shows the percentage of visually breached sensitive data for eight countries. Eighteen percent of German trials resulted in the breach of sensitive data. In comparison, 30 percent of French and U.S. trials resulted in the breach of sensitive data.

Figure 15. Percentage of visually breached sensitive data, by country
Global average (baseline) = 27%
n = 613 pieces of data

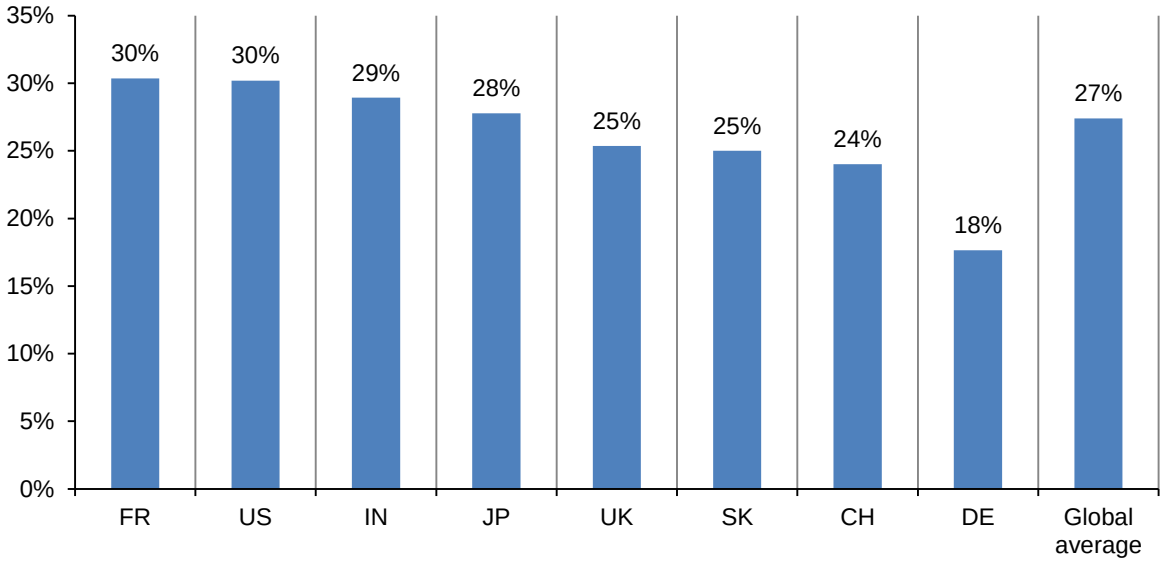


Figure 16 shows four sensitive data types visually hacked in our experiment by country sample. As shown, login credentials to access corporate systems or mobile-connected devices represented the largest sensitive data category for all countries. In contrast, attorney-client privileged documents represented the smallest sensitive data category.

Figure 16. Sensitive data types by country
n = 613 pieces of data

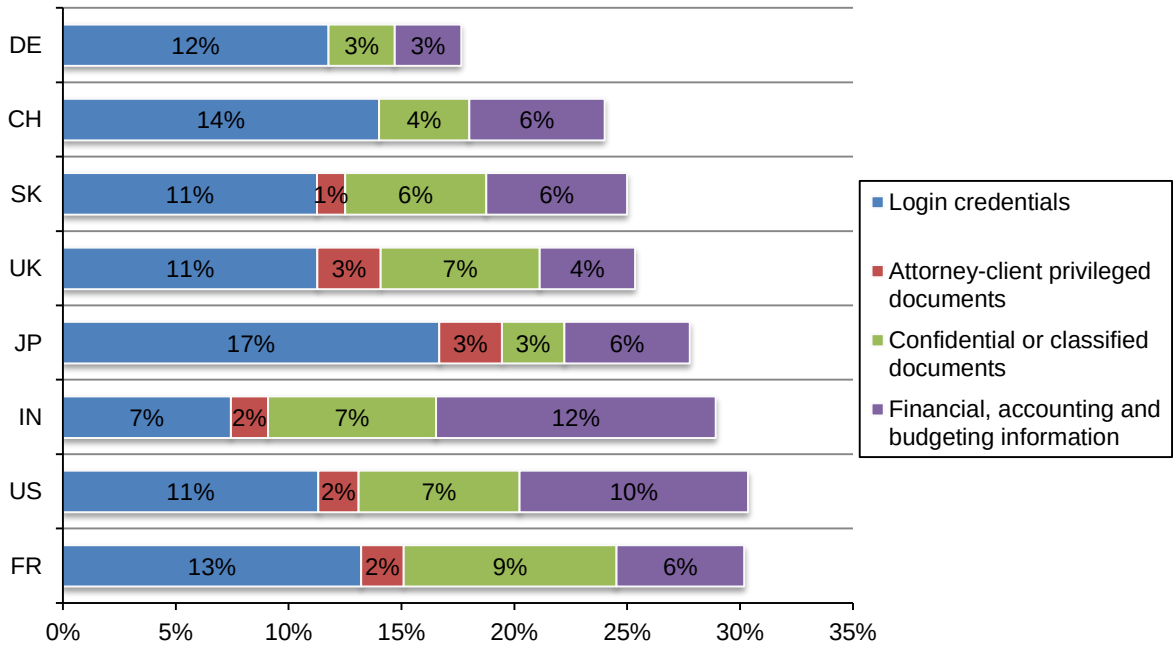


Figure 17 shows the approximate location where the hack occurred during our experiment. Fifty-two percent of sensitive data was captured by observing unprotected computer screens. In comparison, only 28 percent of all breached data occurred by observing computer screens. Forty-nine percent of all data was captured by observing documents on a vacant desk. Only 30 percent of sensitive data was observed from documents on employee desks.

Figure 17. Where visual hacking took place: A comparison of high value vs. overall breached data
n1 = 613 pieces of data, n2 = 168 pieces of sensitive information; 8 countries (combined)

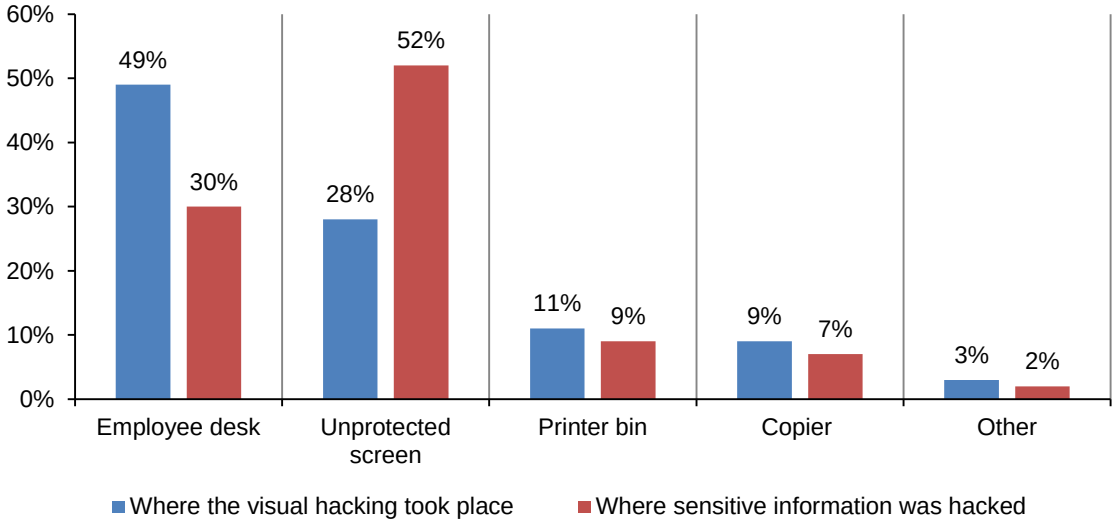


Figure 18 shows country differences in the amount of sensitive information captured from unprotected screens such as laptops, desktops, tablets and smartphones. The pattern of country-level results suggest Korean respondents are most likely to experience the leakage of sensitive information from unprotected screens. Overall, 52 percent of sensitive data leakage occurred from unprotected screens.

Figure 18. Percentage of sensitive information visually hacked from unprotected screens by country

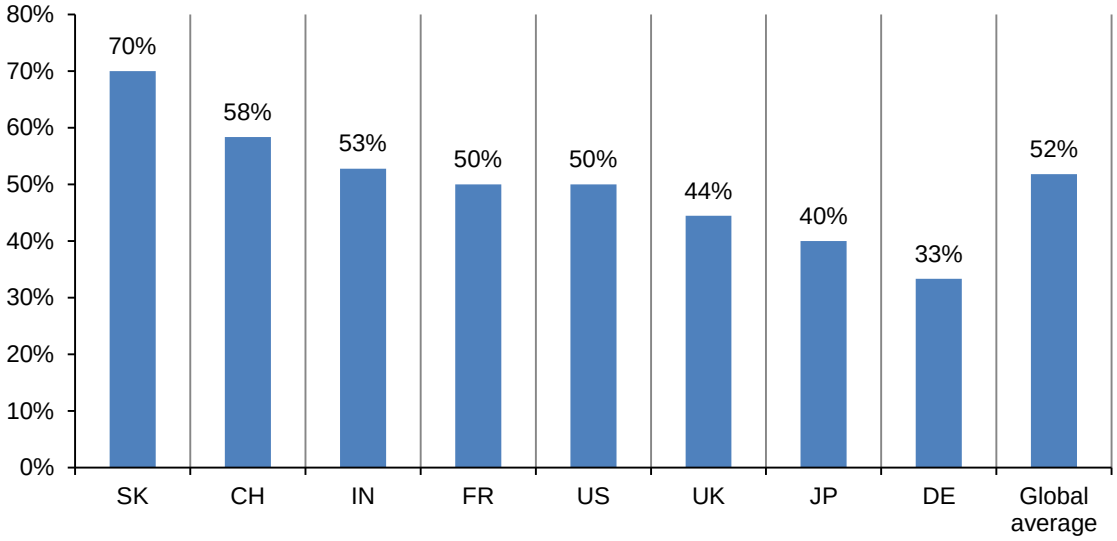


Figure 19 reports that 49 percent of all trials experienced the first visual hack within 15 minutes of the session. Another 17 percent experienced the first visual hack within 15 to 30 minutes. As previously noted, 9 percent withstood a visual hack.

Figure 19. Elapsed time to complete first visual hack
n = 157 trials; 8 countries (combined)

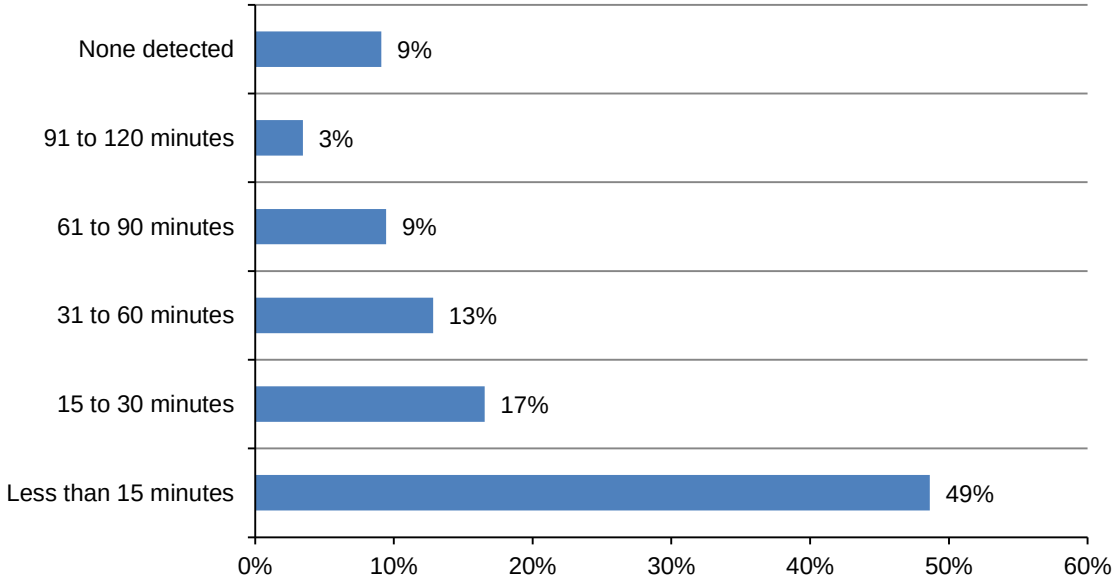
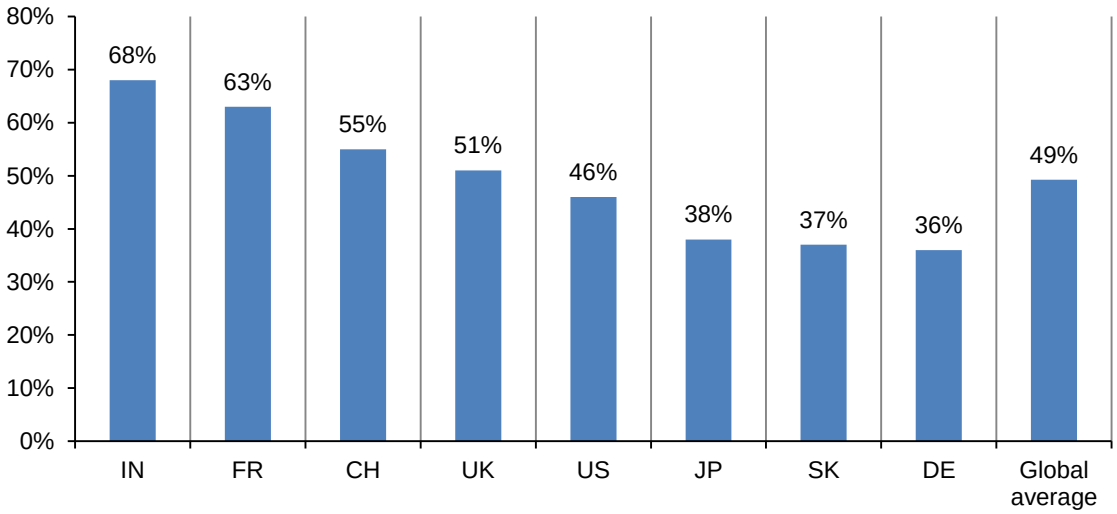


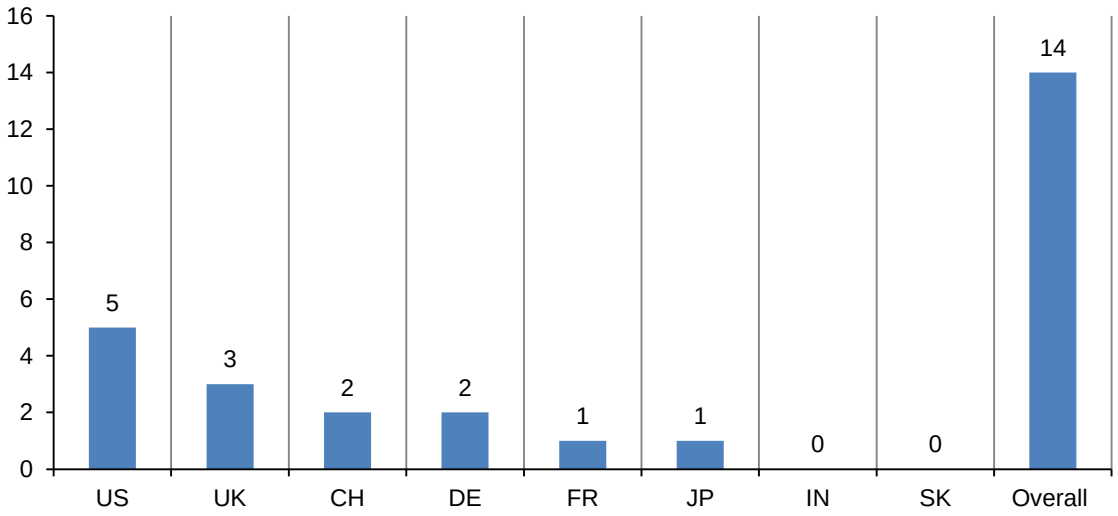
Figure 20 reports the percentage of all trials by country that experienced the first visual hack in first 15 minutes of the session. At 36 percent, Germany experienced the lowest rate of successful hacks within the first 15 minutes of the experiment. At 68 percent, India experienced the highest rate of successful hacks during the first 15 minutes.

Figure 20. Percentage of trials where first visual hack occurred within 15 minutes, by country
Global average (baseline) = 49%
n = 157 trials



According to Figure 21, the hacker was unable to visually hack the company in only 14 cases. None of the experimental trials conducted in India and Korea were hack-free.

Figure 21. Number of trials that were not visually hacked by country
n = 157 trials



As shown in Figure 22, 91 percent of visual hacking attempts were successful – detecting no visual hacks in only 9 percent of all cases. At 82 percent, China had the lowest success rate.

Figure 22. Visual hacking success rate by country
n = 157 trials

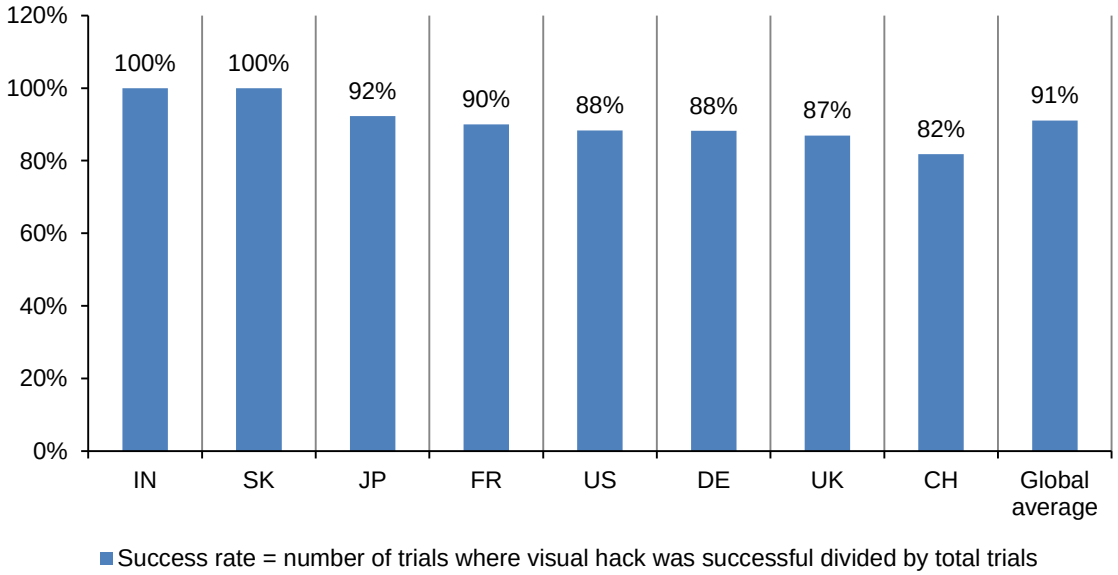


Figure 23 shows that in 107 experimental trials (68 percent), office workers did not confront the researcher. In 50 (30+12+8) trials, the researcher experienced some queries or pushback by some office workers at different points in the session. In only three cases did an office worker contact the office supervisor or manager (liaison) about a possible insider threat.

Figure 23. Did office workers confront the visual hacker?
n = 157 trials

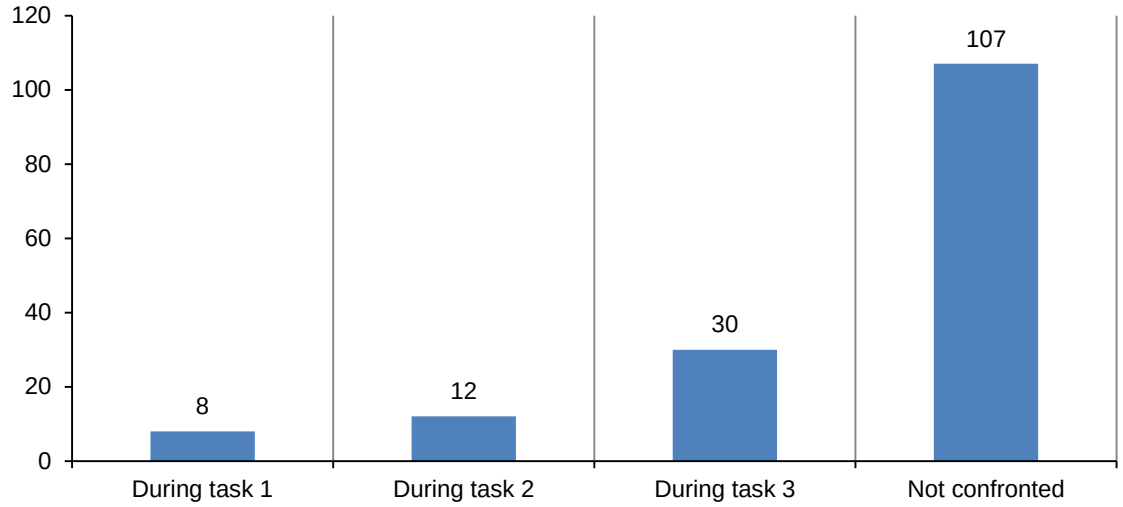


Figure 24 shows the percentage of trials where the visual hacker was not confronted by office workers. For 59 percent of trials conducted in Germany, there was no confrontation between office workers and the visual hacker. In other words, for 41 percent of German trials, there was some interaction between office workers and the hacker. In contrast, for 80 percent of trials conducted in France, there was no interaction.

Figure 24. Percentage of trials where the visual hacker was not confronted by country
Global average (baseline) = 68%
n = 157 trials

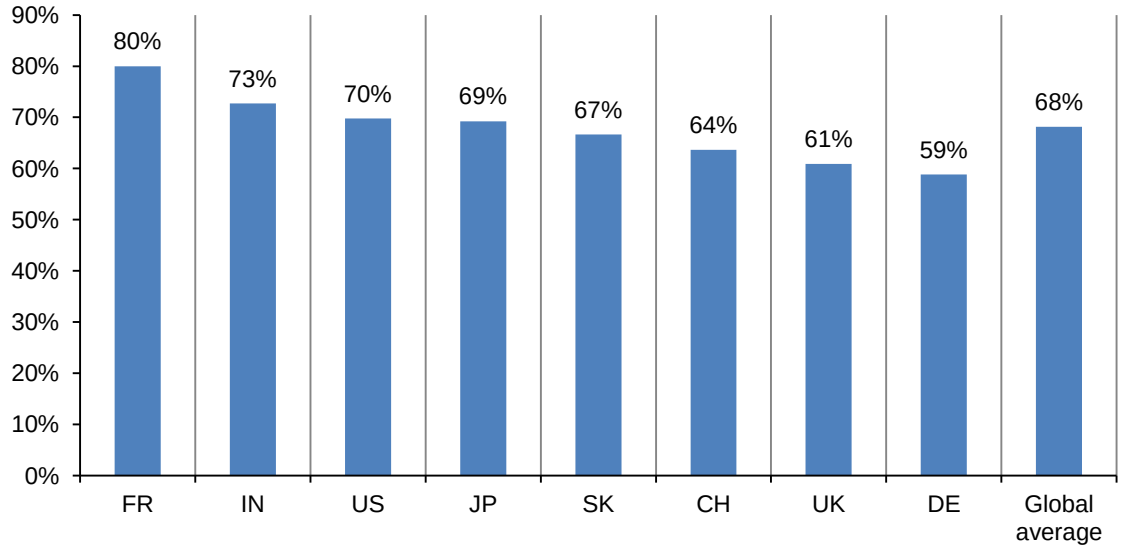


Figure 25 suggests a relationship between visual privacy breaches and the layout of the office involved in the experimental trial. Open layout refers to a design that does not separate office workers. All walls or cubicles are removed. A total of 65 trials (41 percent) were conduced in an open layout and 92 trials (59 percent) in a traditional office layout. In the trials conducted in an open office layout, the average number of visual privacy breaches was 4.5. For trials conducted in a traditional office layout, the average number was 3.2. Hence, the open layout appears to have increased the ability of the visual hacker to observe and obtain company-specific information.

Figure 25. Average number of visual privacy breaches by office layout
n = 157 trials

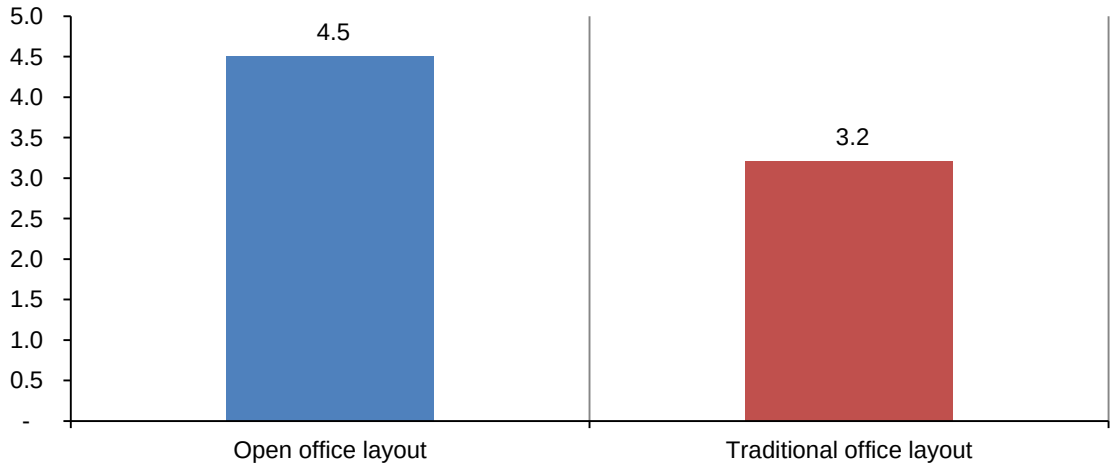


Figure 26 reports the average number of visual privacy breaches for organizations that deploy each one of four common control practices versus organizations that do not deploy these controls. Companies that deploy workplace monitoring averaged 3.2 breaches versus 4.6 breaches for companies that do not deploy this control. Similarly, companies that have a privacy or data protection training and awareness program for employees averaged 3.3 breaches as compared to 4.5 breaches for companies that do not provide training for employees.

Figure 26. Companies with sound control practices experience fewer visual privacy breaches
n = 157 trials; 8 countries (combined)

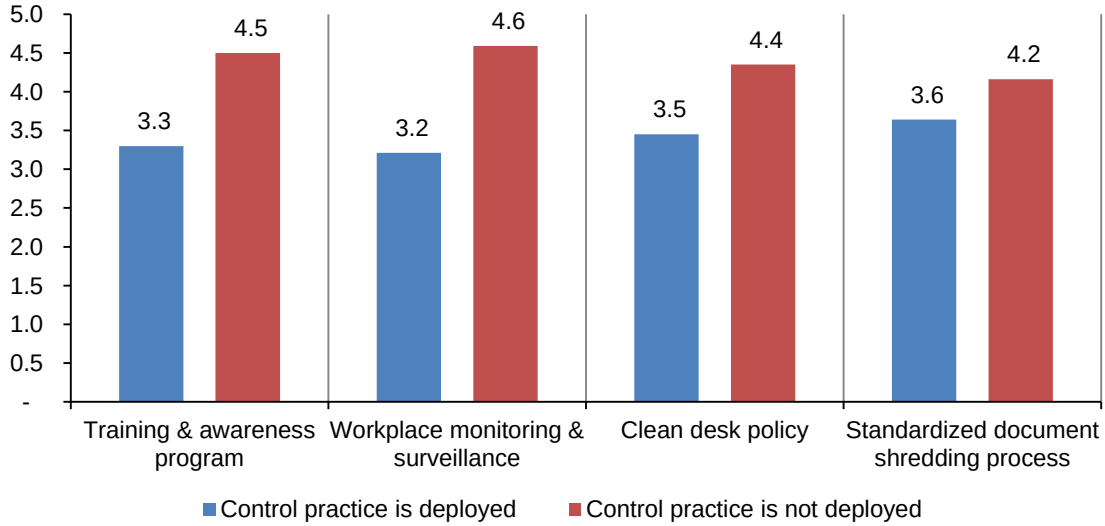
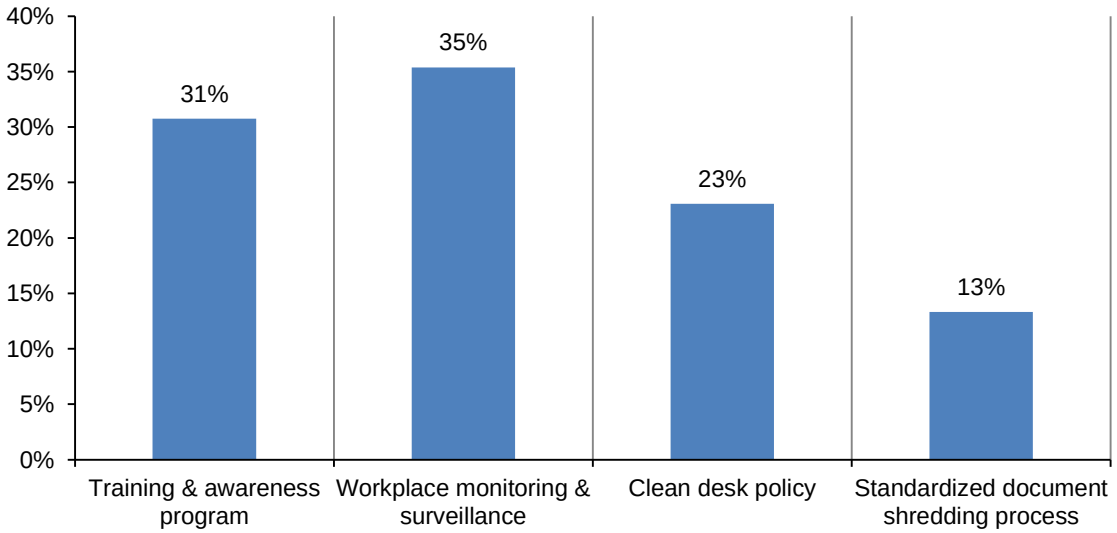


Figure 27 shows the percentage difference in the average number of visual privacy breaches for companies that deploy each one of four control practices versus organizations that do not deploy these practices. For instance, companies that deploy workplace monitoring and surveillance experienced 35 percent fewer visual data breaches than companies that do not monitor employees. Companies that train employees on privacy and data protection had 31 percent fewer visual data breaches than companies that do not conduct privacy or data protection training.

Figure 27. Percentage difference between companies that deploy or not deploy four control practices
n = 157 trials; 8 countries (combined)



Part 4. Implications and Recommendations

According to the findings of the research, visual hacking in the workplace poses a serious risk to an organization's sensitive and confidential information. Following are the implications of this research:

- For reasons of productivity and a more egalitarian working environment, many organizations are migrating from the traditional configuration of private offices and cubicles to open workspaces. An unintended consequence is the difficulty of keeping paper documents and computer screens from being viewed by visual hackers. Organizations should assess the risk of this new office environment to sensitive information.

- Visual hacking is pervasive and occurs in all industry sectors and at all levels of an organization. Where sensitive and confidential information resides so does the risk of a data breach. Therefore, all organizations should institute a visual privacy policy that outlines the specific actions, procedures and best practices to prevent the display of important data in plain sight.

- Often employees and contractors are not aware that the information they work with is desirable to visual hackers. As a result, they often do not take appropriate safeguards to prevent such information from being on open display. Training and awareness programs should be an integral part of an organization's security and privacy strategy.

- Visual privacy is a security threat that is often invisible to senior management. While organizations are increasing budgets for enabling security technologies, resources to support a stronger visual privacy strategy are often not made available.

- Organizations should assess whether employees and contractors have too much access in their workspaces and in off-site locations to sensitive and confidential information. Limiting access to sensitive information without reducing productivity can help reduce the risk of a potential data breach.

Part 5. Limitations

There are inherent limitations to experimental research that need to be carefully considered before drawing inferences from the findings presented here. The following items are specific limitations that are germane to most field-based experimental studies.

Findings are based on a voluntary sample of 46 participating companies and 157 unique office locations in eight countries. Invitations were sent to a representative sample of individuals in a variety of functional areas. We acknowledge it is possible that companies who did not participate are substantially different in terms of their preparedness for visual hacking incidents.

The accuracy of experimental results is dependent upon the researcher's ability to create situations that represent the underlying phenomenon of interest. The degree to which our experiment did not capture a visual hack could not be measured.

The quality of experimental research is based on the integrity of confidential responses received from subjects. While certain checks and balances were incorporated into our research design process including sanity checks, there is always the possibility that some trials did not reveal accurate results.

A final limitation of this study concerns the inclusion of U.S. results that were captured more than 18 months before the other country-level experimental studies were conducted. While unlikely, it is possible that external events during this 18-month time gap could have influenced the study results.

Please contact research@ponemon.org **or call us at 800.887.3118 if you have any questions.**

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.