3M Visual Hacking Experiment

Sponsored by 3M and the Visual Privacy Advisory Council

Independently conducted by Ponemon Institute LLC

Publication Date: February 2015

Visual Hacking Experimental Study

By Ponemon Institute, February 2015

Part 1. Introduction

Ponemon Institute is pleased to present the results of the *Visual Hacking Experimental Study*, sponsored by 3M and the Visual Privacy Advisory Council (VPAC). The VPAC is a group of data privacy and security thought leaders dedicated to raising awareness of this issue and promoting best practices and policies to prevent costly visual hacking attacks.

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 and smartphones as well as in paper documents that are left in plain sight on desks, printers, conference tables, and other office locations or outside meeting sites.

As the findings reveal, a visual privacy policy is important to creating awareness among employees of the need to protect sensitive information from visual hackers. Such a policy outlines the specific actions, procedures and best practices an organization requires from employees to prevent the display of important data that is in clear view of potential hackers.

Visual hacking is easy. Eighty-eight percent of the visual hacking attempts were successful.

A company's most valuable information assets are at risk. Twenty percent of the data hacked was considered a very valuable information asset.

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

Visual hacking is fast. It took less than 15 minutes to complete a visual hack in 45 percent of the hacking attempts.

People are timid about confronting a visual hacker. In 70 percent of the hacking attempts, office personnel did not question or report the visual hacker even after witnessing unusual or suspicious behavior.

Open office floor plans are ideal for visual hacking. Traditional offices and cubicles make it easier to protect paper documents and more difficult to view a computer screen. This can minimize the risk of visual hacking.

How serious is the risk of visual hacking? A previous study conducted by Ponemon Institute[1] dispelled the myth that the cause of most or all data breaches involves lost or stolen electronic documents. In this study, 80 percent of respondents who self-reported their organizations had at least one data breach in a 12 month period said that 49 percent of these breaches involved the loss or theft of paper documents.

In fact, 71 percent of participants in the study were aware of an incident in which sensitive or confidential paper documents were lost or misplaced in their organization. Moreover, 53 percent believed that employees are putting them at risk at communal printers, in meeting rooms or at meetings held outside the office. 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 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 strict policy for securing paper documents both within the office and at offsite 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.

[1] *Security of Paper Documents in the Workplace*, conducted by Ponemon Institute and sponsored by the Alliance for Secure Business Information, October 15, 2008.

Part 2. Experimental Methods

Ponemon Institute conducted a "white hat" experiment involving actual visual hacking in real workplace settings. Our mission was to test organizations' readiness to prevent and detect visual hacking in the business office environment. Ponemon Institute's benchmark community members were contacted for participation in this research.[2] More than 100+ companies representing 16 industry sectors were invited.

We recruited 8 U.S.-based companies that allowed us to field our experiment within actual office locations. As noted in Table 1, a total of 43 trials were conducted over a two-month period ending in July 2014. By design, all field experiments occurred on premises during the normal workday.[3]

Table 1. Recruited companies	Trials	Pct%
Global financial services	8	19%
IT services	8	19%
Automobile manufacturer	6	14%
National banking	6	14%
P&C insurance	5	12%
Life sciences	4	9%
Research & education	3	7%
Defense & aerospace	3	7%
Total	43	100%

Table 2 shows 10 functional areas that provided the venues for this study. The largest functional areas were customer services, sales management and data center operations.

Table 2. Functional areas	Freq	Pct%
Customer services	10	23%
Sales management	7	16%
Data center operations	6	14%
Human resources	6	14%
Accounting & finance	5	12%
Help desk	2	5%
Logistics	2	5%
Communications	2	5%
Legal	2	5%
R&D	1	2%
Total	43	100%

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 including 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.[4] 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 per location. To preserve confidentiality, the actual information

[2]This benchmark community consisted of 1,208 organizations at the time of this study.
[3]In most cases, participating companies used experimental results as part of training and awareness efforts.
[4]The company liaison was a supervisor or manager located in each office where the experiment was conducted. This individual was given explicit instruction by the researcher approximately two weeks before the experiment on the purpose of the research and the need for secrecy.

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:[5]

- 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

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 scouting 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 smart phone's digital camera to take pictures of what appeared to be business confidential information on the computer screen or terminal.

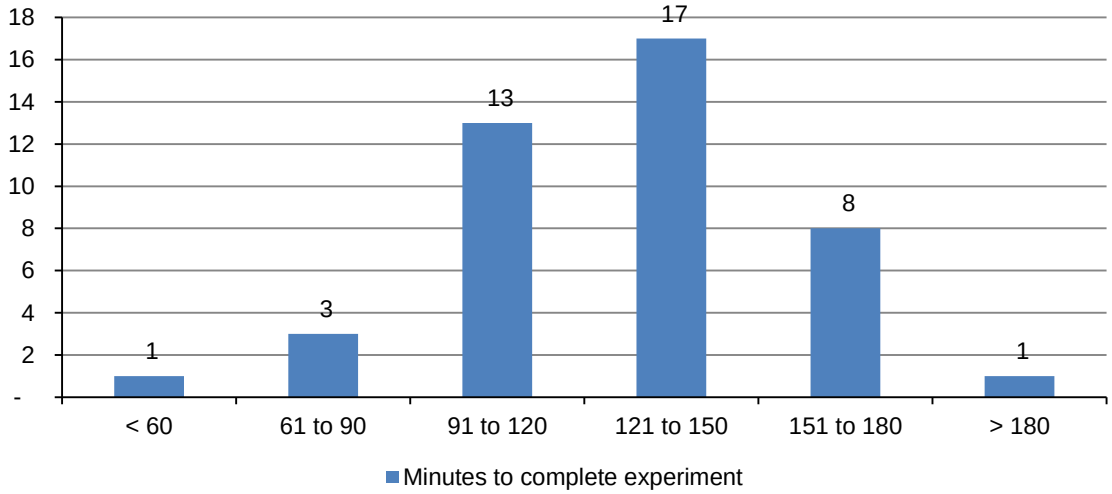
Debrief: At the conclusion of all three tasks, the company liaison and researcher conducted a debriefing session with office workers located in the area of the experiment to determine their perceptions and level of awareness about visual hacking. Did these office workers recognize this as a suspicious 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 researcher was instructed not to perform extra-ordinary tasks to observe documents or displayed data. Hence, the researcher relied solely upon causal observation to record information types.

Part 3. Key Findings

The average total time to complete all three experimental tasks was 127 minutes (not including the debriefing session). Figure 1 provides the time distribution for 43 experimental trials.

Figure 1. Histogram on the minutes to complete three experimental tasks
(n = 43 trials)



A total of 168 instances of visually hacked information occurred in 43 experimental trials (or an average of 3.9 instances per trial). Figure 2 provides the percentage frequency of information types visually hacked in this study. The information type most frequently hacked concerns contact lists and directories (including employee directories). At 1 percent, attorney-client privileged information is the least likely to be visually hacked in this experiment.

Figure 2. Percentage frequency of information types visually hacked
n = 43 trials

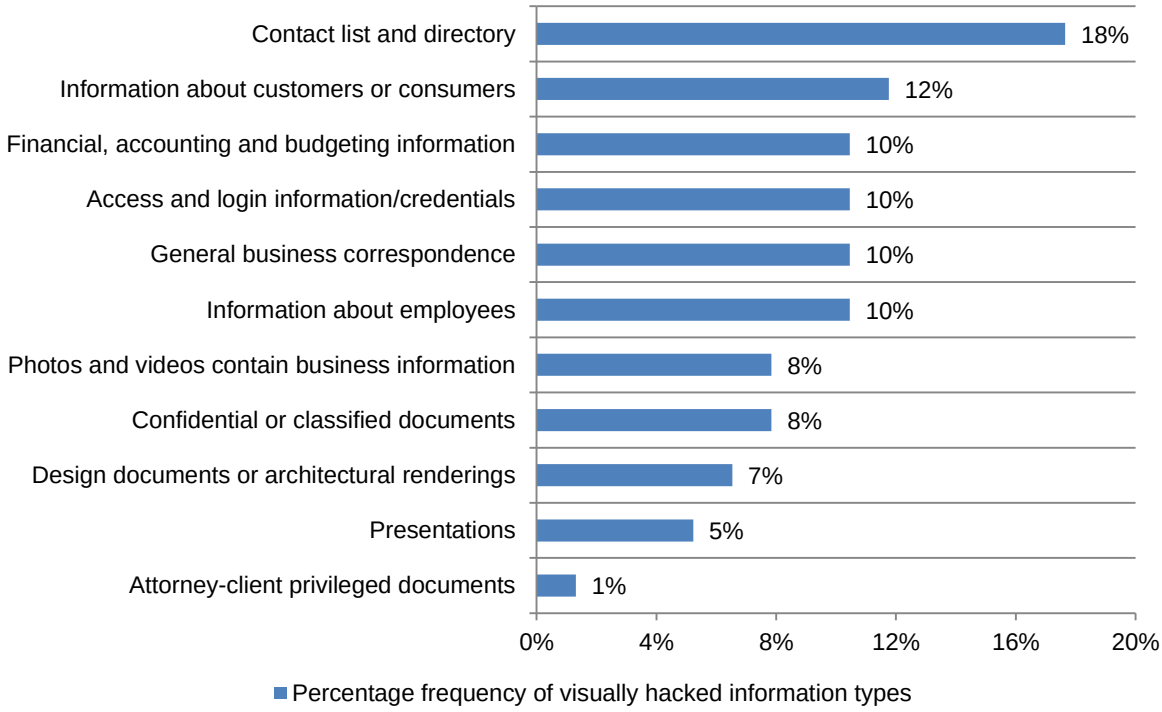


Figure 3 reports the frequency distribution for the number of information types observed by the researcher for all 43 experimental trials. As can be seen, five trials (or 12 percent) did not experience visual hacking.[6] In other words, over 88 percent of experimental trials experienced at least one instance of visual hacking. Six of 43 trials experienced more than six information types observed by the researcher.

Figure 3. Histogram of information types captured
n = 43

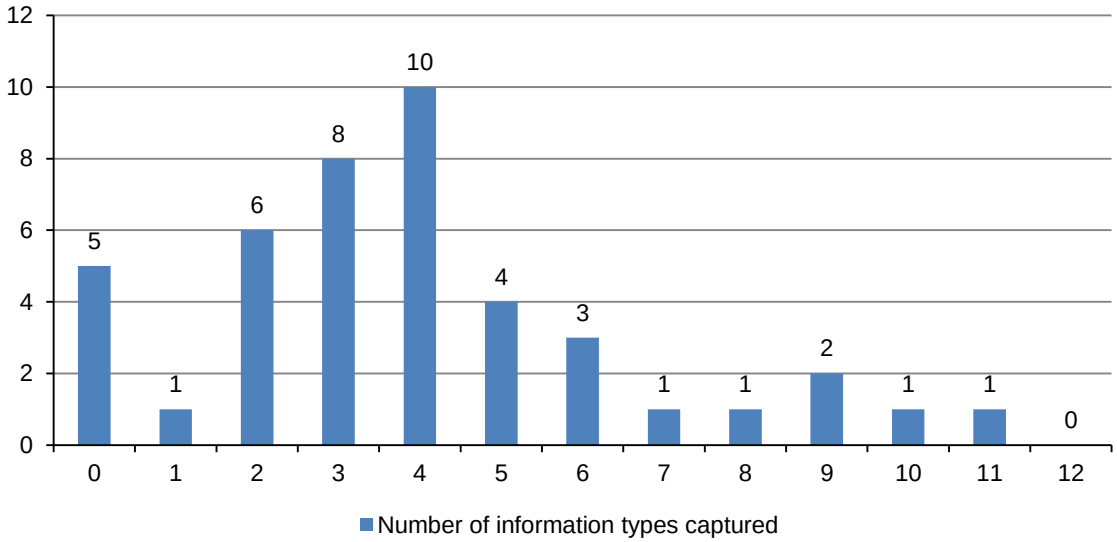
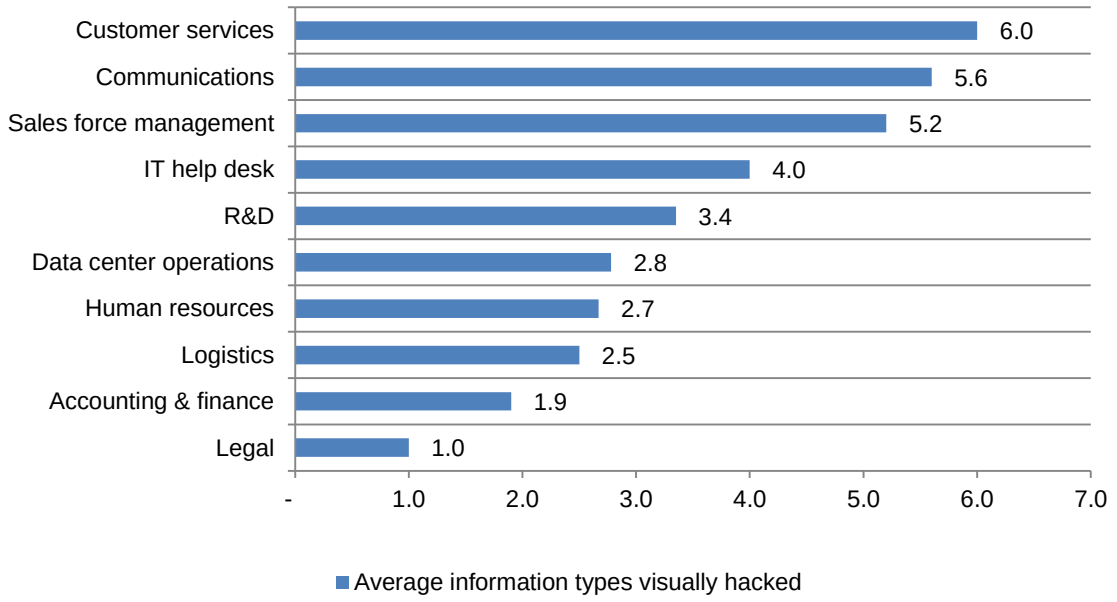


Figure 4 shows significant variation among functional areas. Experimental trials conducted in customer services or corporate communications appear to have the most information types visually hacked. In contrast, legal has the least number of information types visually hacked.

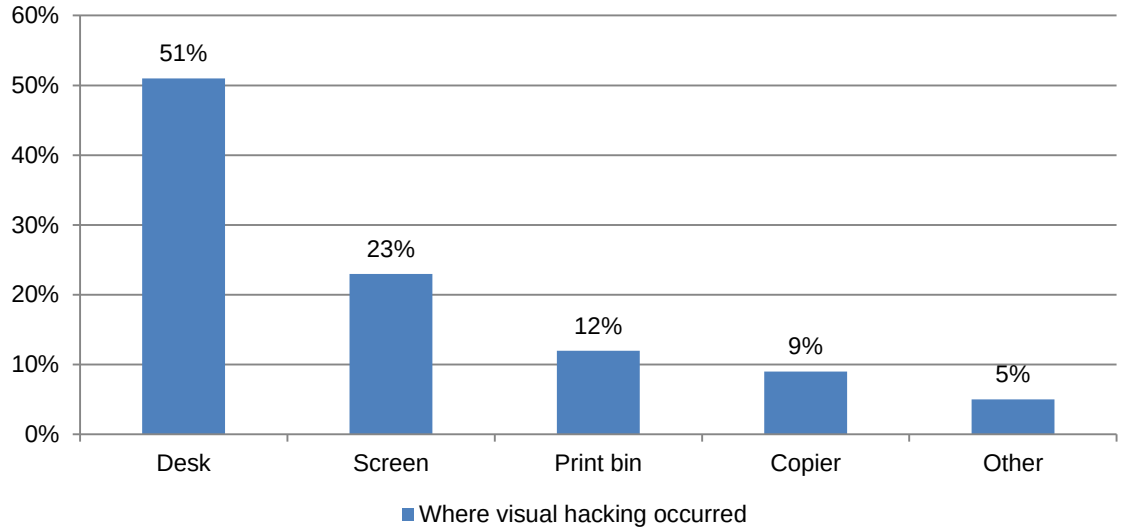
Figure 4. Average number of information types visually hacked by functional area
n = 43 trials



[6]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.

Figure 5 summarizes the location where sensitive or confidential information was observed by the researcher. As can be seen, 51 percent of all visual hacks involved documents visible on desks. Another 23 percent of visual hacks involved information gleaned from unprotected desktops, laptops, tablets and other mobile devices.

Figure 5. Where the visual hacking occurred for all information types
n = 43 trials



Of all 168 pieces of captured information, 34 pieces (20 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 6. Proportion of sensitive information
n=43 trials

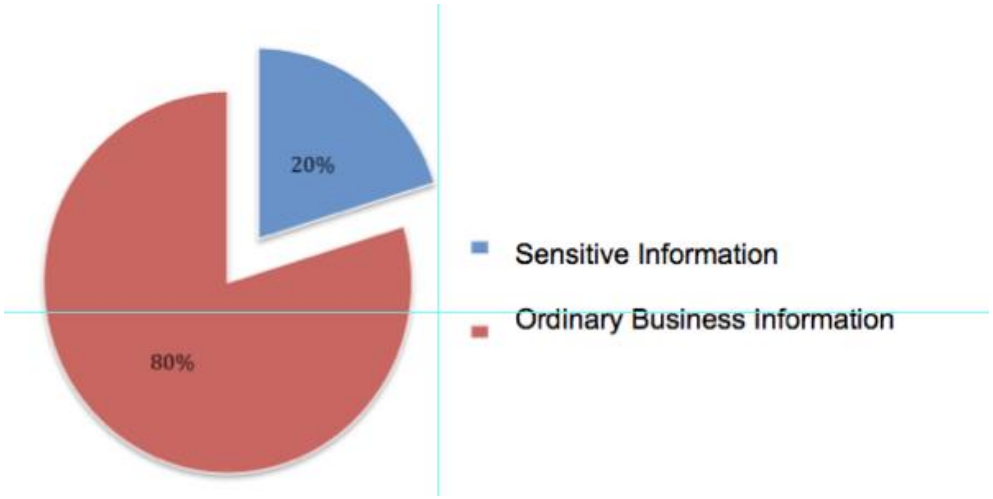


Figure 7 lists four sensitive information types visually hacked in our experiment. As shown, 47 percent of this information pertained to access and login information such as credentials to access corporate systems or mobile-connected devices. Thirty-five percent pertained to documents marked confidential or classified. Another 12 percent pertained to non-public financial information, and 6 percent to attorney-client privileged documents.

Figure 7. Sensitive information types
n = 43 trials

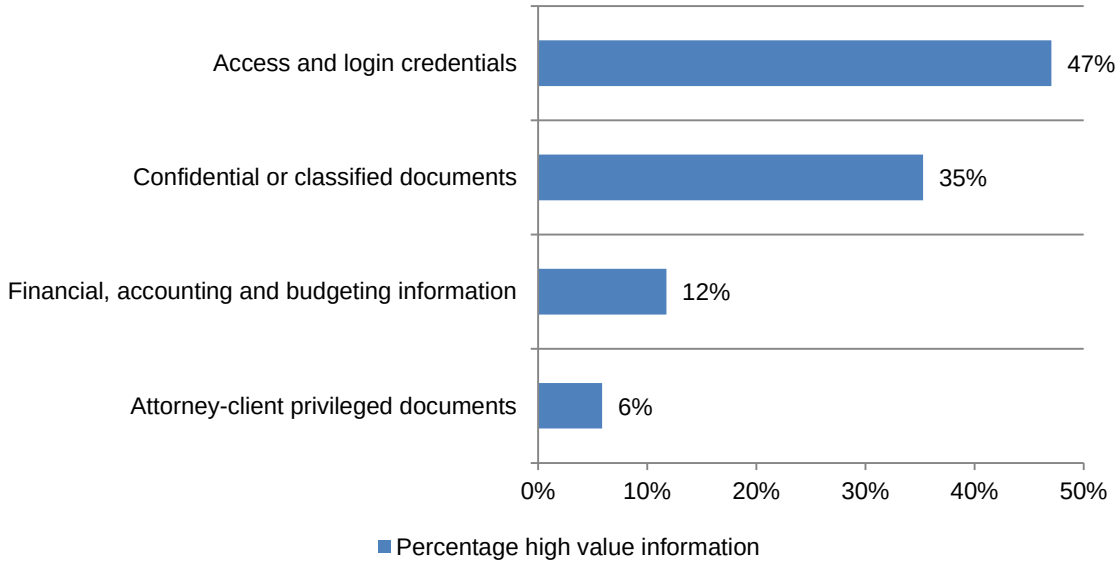
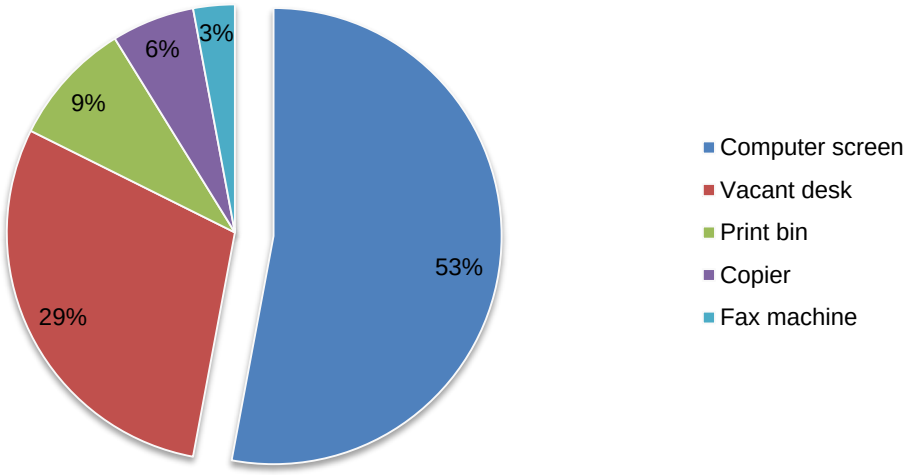


Figure 8 shows the approximate location where the hack occurred during our experiment. Fifty-three percent was captured by observing unprotected computer screens.[7] In addition, 29 percent of this information was observed from documents on vacant desks. The remaining locations include printers (9 percent), copiers (6 percent) and fax machine (3 percent).

Figure 8. Locations where sensitive information assets were hacked
n = 43 trials



[7]It is interesting to note that the percentage of hacks from observing computer screens varied significantly between ordinary and sensitive information types. Accordingly, only 23 percent of all information types were hacked from observing computer screens on desktops, laptops and tablets.

According to Figure 9, 19 trials (45 percent) experienced the first visual hack within the first 15 minutes of the session. Another 8 experimental trials (18 percent) experienced the first visual hack within 15 to 30 minutes. As previously noted, 5 trials (12 percent) did not experience a visual hack.

Figure 9. Elapsed time to complete first visual hack
n = 43 trials

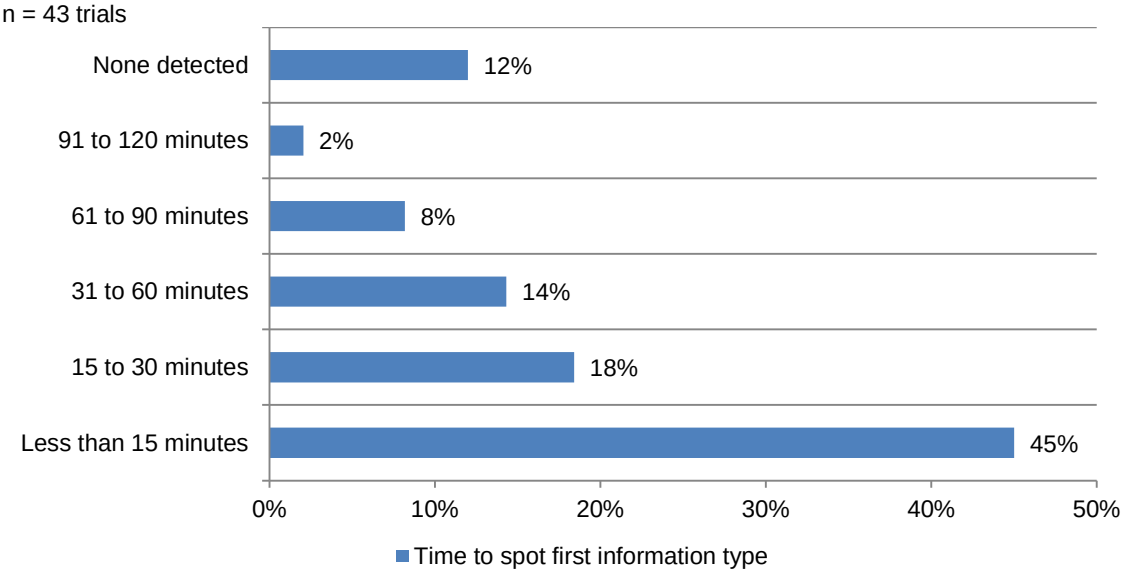


Figure 10 shows in 30 experimental trials (70 percent) the researcher was not confronted by office workers. In 13 trials (30 percent), the researcher experienced some queries or pushback by some office workers at different points in the session. In only one case (during Task 3), the office worker contacted the office supervisor or manager (liaison) about a possible insider threat.

Figure 10. Did office workers confront the visual hacker?
n = 43 trials

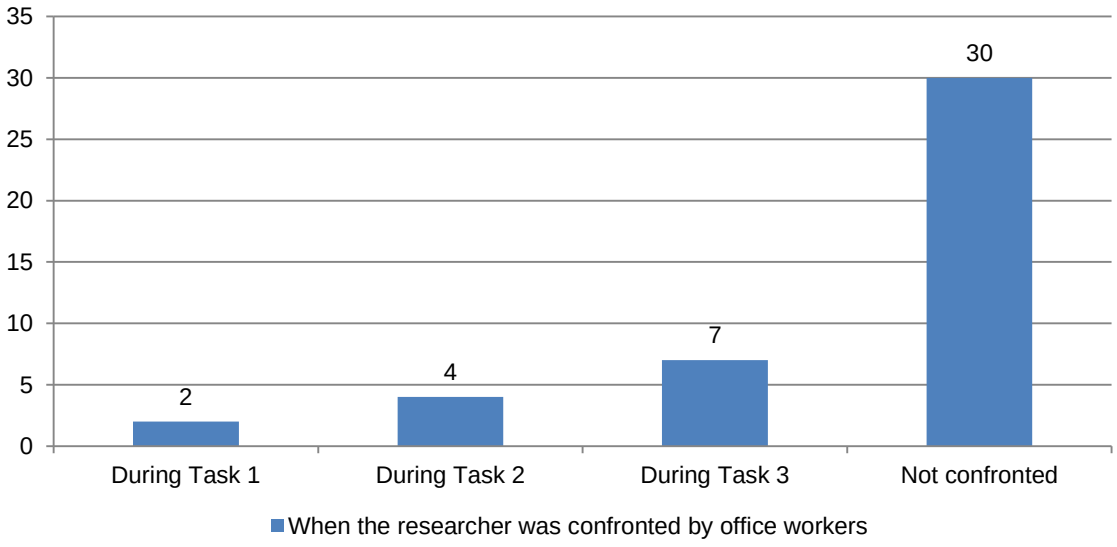


Figure 11 shows a relationship between information types visually hacked and confrontation by office workers during the experimental trial. As reported, in the 13 cases where the researcher was confronted, the average trial produced 2.8 information types. For 30 cases where the researcher was not confronted, the average trial produced 4.3 information types.

Figure 11. Average information types visually hacked by confrontation
n = 43 trials

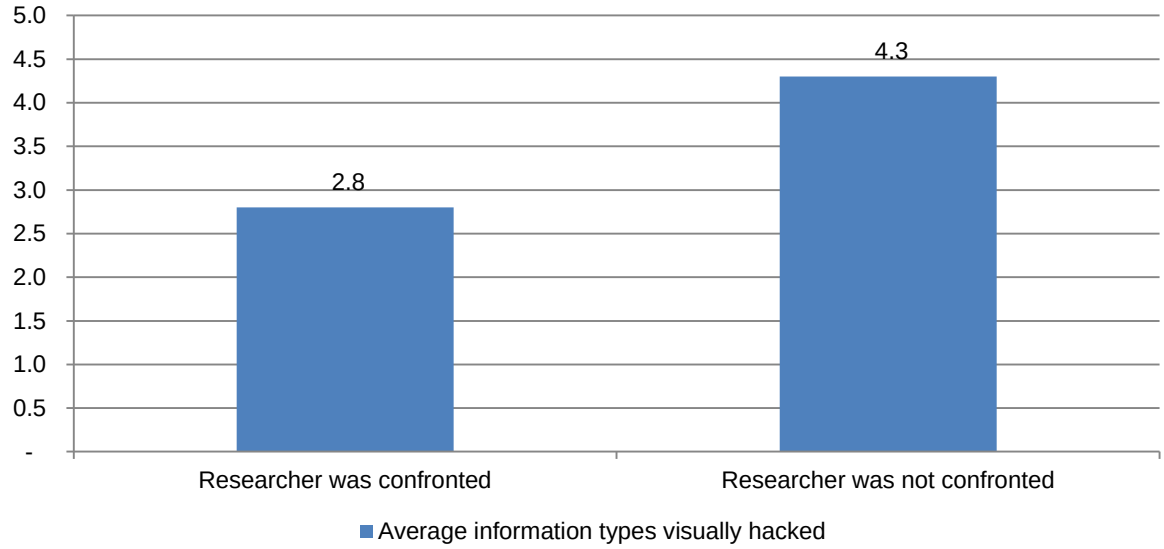


Figure 12 suggests a relationship between information types visually hacked and the layout of the office involved in the experimental trial. The open layout refers to a design that does not separate office workers. All walls or cubicles are removed. A total of 15 trials (35 percent) were conduced in an open layout and 28 trials (65 percent) in a traditional office layout. In the 15 cases conducted in an open office layout, the average trial produced 4.4 information types. For 28 cases conducted in a traditional office layout, the average trial produced 3.0 information types. Hence, the open layout appears to increase the ability of the visual hacker to observe and obtain sensitive or confidential information.

Figure 12. Average information types visually hacked by office layout
n = 43 trials

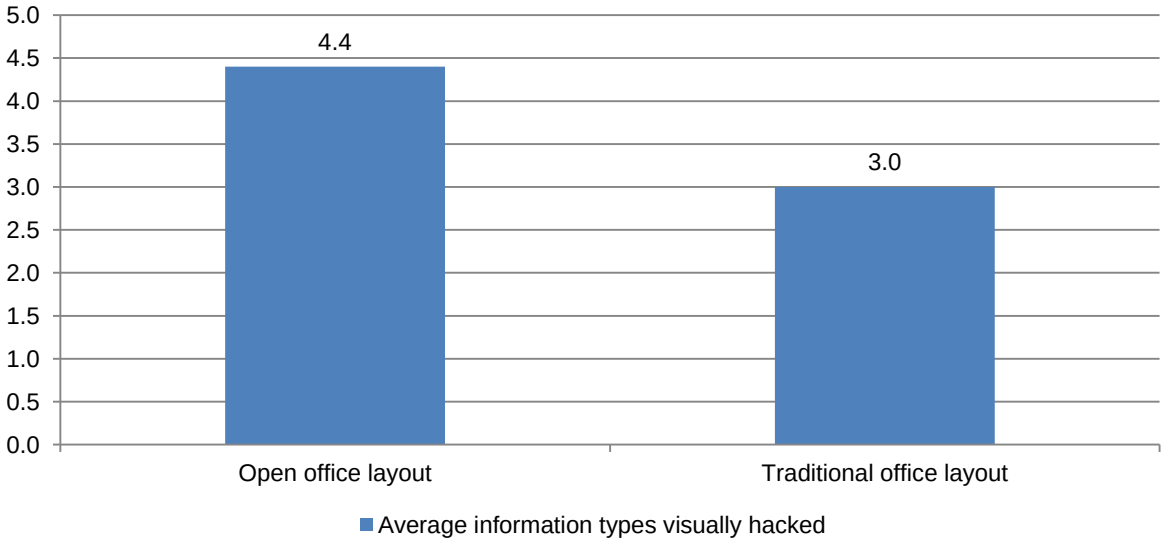
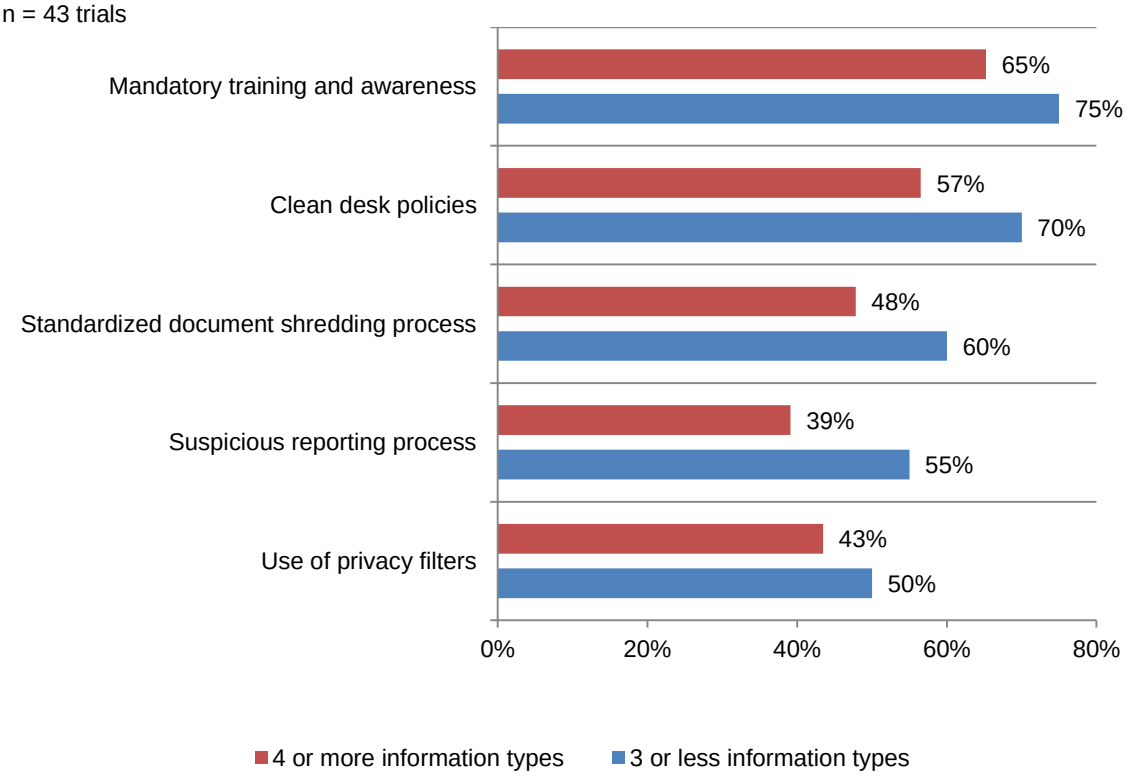


Figure 13 split the 43 trials into two groups – namely, those with a relatively low and those with a relatively high visual hacking rate. The low group had 20 trials with three or fewer hacked information types. The high group had 23 trials having four or more hacked information types. As can be seen, the low group outperformed the high group on five visual privacy control points.

Figure 13. Five salient controls over visual hacking
n = 43 trials



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 in 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 virtual 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 offsite 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 needs to be carefully considered before drawing inferences from the presented findings. The following items are specific limitations that are germane to most field-based experimental studies.

Findings are based on a voluntary sample of 8 participating companies and 43 unique office locations throughout the United States. 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 readiness to 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.

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.