New Study Identifies Visual Privacy As Weak Link in Data Security Practices

Visual Privacy — the protection of sensitive information as it is displayed on screen — is an emerging issue in information security and an under-addressed area of risk in corporate security policies. Given the rapid digitization of sensitive information and the growing mobility of workers, the need to protect displayed information has grown substantially.

The IT analyst firm IDC estimates that over 72% of workers in the United States have some level of mobility[1]. With corporate data being accessed in public places by a wide range of devices (such as laptops, tablets and smart phones), this presents new challenges for businesses that must safeguard information.

The ***Visual Data Breach Risk Assessment Study***, authored by Dr. Hugh Thompson, Chief Security Strategist of People Security, and commissioned by 3M, the makers of computer privacy filters and mobile privacy screen protectors, found a significant risk of data exposure while information is displayed on laptop screens in public environments with correspondingly little security controls in the way of technology and policy to address this risk.

Here is an overview of some other key findings revealed in the Visual Data Breach Risk Assessment Study:

Employees Putting Information at Risk of Visual Data Breach

There is a basic expectation, and in some cases a mandated requirement, that companies keep sensitive information secure at all times – while it is stored, transmitted and viewed. However, the study revealed that two-thirds (67%) of employees expose sensitive data outside the workplace – some even exposing highly regulated and confidential information like customer credit card and social security numbers. With few companies having concrete policies in place to control the type of data employees access outside of the office, there is a significant corporate risk of a visual data breach.

67% of employees expose sensitive data outside the workplace

Smart Phone Camera New Tool for Data Thieves

With employees repeatedly putting regulated customer information and confidential corporate information at risk outside of the office, and cloud-based services now enabling on-demand access of information to working professionals across multiple devices, there are even more opportunities for onlookers or competitors to observe sensitive information. The rise in quality smart phone cameras now makes it possible for a data thief to capture readable information as it is displayed on screen. Since the pictures can now be preserved for future use this increases the risk of a visual data breach.

Visual Privacy Under-Addressed by Corporate Policy

There is a significant gap between risk and corporate policy to prevent visual data breaches. According to the study, 70% of working professionals said their company had no explicit policy on working in public places and 79% said that their company had no policy on the use of privacy filters. This indicates either a lack of attention to visual privacy at the policy level or a failure to effectively communicate policies to employees. Considering that half of the working professionals work on their laptop in a high-traffic public area at least one hour per week, the lack of policy and education around visual privacy creates a significant enterprise risk.

- over -

[1] IDC Worldwide Mobile Worker Population 2009–2013 Forecast, http://www.idc.com/getdoc.jsp?containerId=221309

Employees Value Convenience Over Privacy

While many say they value visual privacy, they may not act to preserve it when it comes to corporate data, creating an operation security risk. Eighty percent of working professionals thought that prying eyes posed a risk to their companies. Yet a majority chose not to protect their visual privacy when accessing information on an unprotected computer in a high-traffic public area. This further illustrates the need for companies to educate employees on the risk of exposing corporate data and regulated information when working outside of the office in public areas.

Opportunity to Increase Productivity

The ability to access information anytime, anyplace, and on any device means that more people have the opportunity to be productive outside of the office. However, employees would actually be more productive when working in public if they knew their information was properly protected from onlookers. By addressing the issue of visual privacy in corporate policies, as well as giving employees the necessary tools to protect the data they are accessing in public, companies will have the potential to make their mobile workforce even more productive when working outside of the office.

Tools such as privacy filters can help reduce risk of data exposure by blocking the side views of computer screens

Conclusions

The study illustrates a lack of awareness at the corporate and individual levels of the risks associated with visual data breaches and displaying sensitive and regulated information in public areas. Addressing this issue requires a mix of education, policy, and controls. Employees need to be made aware of the risk, but perhaps more importantly, they need to be equipped with strategies to reduce that risk.

Tools such as privacy filters can help reduce risk of data exposure by blocking the side views of computer screens. This limits the number of people that can see information as it is displayed. However, in addition to being given the tools (i.e. privacy filters), employees also need to be educated on the risks of a visual breach and then incented through policy to use these tools.

Lastly, a foundational principle of information security is defense-in-depth — which states that systems should be protected with multiple layers of defense. When applied to data security, a defense in depth approach demands that enterprises have security controls on information as it is stored, transmitted, used and displayed. This study shows that safeguarding displayed data is an under-addressed area in IT security and may be a weak link in the lifecycle of sensitive data. Tools and policies to safeguard information as it is displayed need to be a part of any effective enterprise information security strategy.

Key Findings

Types of Sensitive Data Worked With Outside of the Office

- Social Security Numbers 23.94%
- Credit Card Numbers 26.18%
- Medical Information 15.34%
- Trade Secrets 32.17%
- Internal Financials 41.77%
- Private HR Information 33.17%

Policies on Working in Public Places

- Some corporate roles are restricted from working in public places 3%
- I don't know what my company's policy is 11%
- Work is generally not permitted in a public place 16%
- No explicit policy on working in public places 70%

How Important is Privacy to You?

- Very Important 65%
- Somewhat Important 30%
- Not Very Important 4%
- Not Important at All 1%

Perception vs. Reality Percentage

Q: If two internet kiosk machines were available, one with a privacy filter and one without, which would you use?

- People **who actually chose** a machine with a privacy filter 35%
- People **who said they would choose** a machine with a privacy filter 80%

For more information and full study findings, go to http://www.3Mprivacyfilters.com/whitepapers

3M Privacy Filters