How Exposed is Your Organization? An Enterprise Visual Privacy Maturity Model (VPMM)

With the explosive growth in worker mobility, enterprises are faced with more screens in public places. Some organizations have taken a proactive approach to managing visual privacy — putting policies and controls in place to help manage risk. However, many companies have left the risk unmanaged. During a survey of 800 working professionals, 70% of respondents revealed that their organizations had no explicit policy on working outside of the office. When combined with the fact that 67% of respondents had worked with some type of sensitive data outside the trusted confines of the office within the past year, this indicates a serious gap between the risk and the security controls to manage that risk.

Managing visual privacy requires a combination of policy, education and security controls. In this paper we introduce a Visual Privacy Maturity Model (VPMM) to help calibrate your organization's approach to managing sensitive data that is exposed when it is displayed on a screen. The VPMM has four phases: Unmanaged, Risk Reduced, Risk Controlled and Optimized.

Phase 1: Unmanaged

In the Unmanaged phase, the organization is essentially ignoring the risk of a visual breach and there is no cohesive corporate strategy for visual privacy protection. This phase is characterized by vague policies on working outside the office, limited management of the visual exposure of data, and little to no education for employees on the importance of maintaining visual privacy.

Phase 2: Risk Reduced

In the Risk Reduced phase, some effort has been made to reduce the risk of a visual breach through policy and the use of controls such as screen privacy filters. This phase is characterized by a broad set of policies on working outside the office and the distribution of privacy filters for high risk groups (such as executives). In this phase, privacy filters may be opt-in for certain groups (employees needing to request a filter as opposed to them being proactively supplied). There is no enterprise strategy for educating employees on the risk of a visual data breach although high-risk groups may receive some education.

Phase 3: Risk Controlled

In the Risk Controlled phase, the risk of a visual breach is appropriately managed and the organization is taking steps to control data exposure. Organizations at this phase are grouping employees by exposure risk and enforcing policies to limit the exposure of data by group. Employees are educated on the risks of a visual data breach. This education is integrated into general enterprise security awareness programs, as well as new employee orientation and on-boarding. Controls such as privacy filters are distributed to at-risk groups and their use is enforced among high-risk groups.

67%

percentage of employees expose sensitive data outside the workplace, risking visual data breach.[1]

70%

of working professionals surveyed said their company had no explicit policy on working outside the office.[1]

**Privacy is
the best policy.**

3M

Phase 4: Optimized

In the Optimized phase, the enterprise is leveraging the use of visual privacy controls to increase the mobility and productivity of employees while managing risks. Risk assessments are done for devices used outside of the office as well as devices used inside the office (where data must be protected even from other employees). Employees are risk-stratified by the data they work with as well as the time they spend working outside the office or in shared workspaces. Managers, as well as employees, are educated on the risk of a visual breach, and visual privacy is addressed through add-on controls such as privacy filters, application and work flow architecture. Visual privacy controls, policies and educational components are used as tools to enable employee freedom and productivity. Moving along the path from unmanaged to optimized takes focused effort but is increasingly important. Forecasts predict even more growth in worker mobility. This trend, combined with the rapid digitization of sensitive information and the explosive growth of mobile devices means more work will be done in public places. Managing the risk — and facilitating an agile workforce — will be critical.

An important element of visual privacy defense is the use of screen privacy filters to protect data from unauthorized insiders as well as external observers. By blocking out side views, privacy filters can help reduce the risk of sensitive data exposure. 3M, a leader in privacy protection, offers a range of sizes and styles to protect laptops, desktops and even mobile phones.

For more information on the Visual Privacy Maturity Model and privacy filters in general visit: **http://www.3Mscreens.com.**

3Mscreens.com

[1] Thomson, Herbert H, PhD. "Visual Data Breach Risk Assessment Study" 2010. People Consulting Services.

Privacy is the best policy.