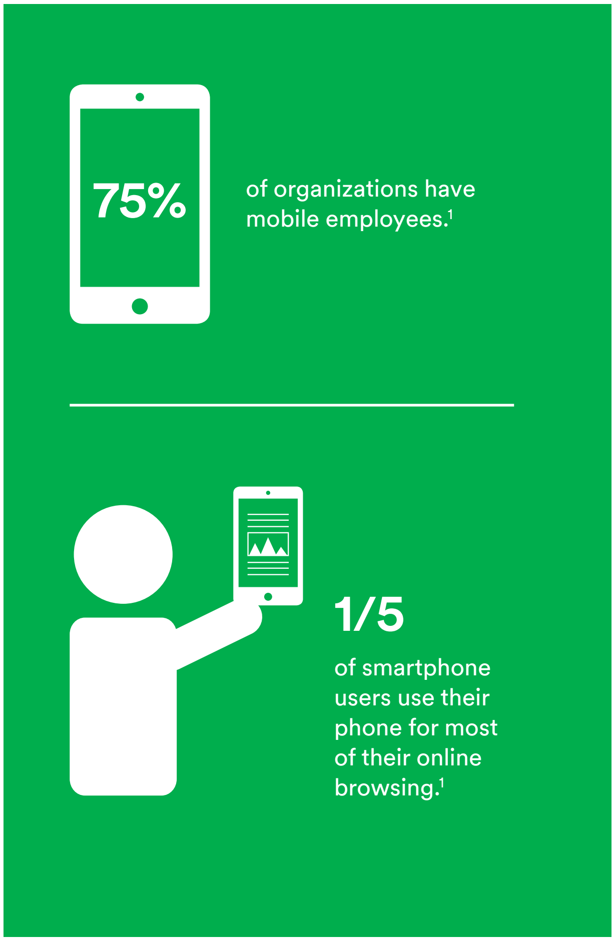
Three In-Practice Approaches to Defending Against Visual Hacking

The increasing mobility of workers, coupled with the growth of cloud-based services that allow access to data any time, anywhere has forced security professionals to re-examine enterprise defense. While controls that protect data when it is stored and transmitted have been widely adopted, the use of controls to protect data as it is displayed and used has fallen significantly behind. One critical area of data-in-use protection is visual privacy, the act of protecting sensitive, confidential and private information from visual hacking, or the act of viewing or capturing sensitive, confidential and private information for unauthorized use. Protecting businesses against visual hacking has become increasingly important given that mobile workers often access data in highly exposed areas such as coffee shops, trains and airplanes.

Despite the increased importance of visual privacy, the IT industry has regressed in this area in some ways. Take the entering of a password into a mobile device at a login prompt for example. This data has traditionally been "masked" when entered — meaning that an onlooker never sees the password characters displayed on the screen as they are typed, thereby reducing the risk of an onlooker capturing that data. Many mobile devices, however, unmask each character entered to improve user accuracy, having the unfortunate side-effect of exposing that data to an onlooker. Beyond passwords, employees in the field routinely access sensitive data outside the trusted confines of the office. These changes in how work gets done in public places means that enterprises need to rethink their security strategy to include the protection of data as it is displayed. This paper looks at three in-practice approaches — from a technology provider, a manufacturing company and a regional bank — for integrating visual privacy controls into enterprise security strategies.



75% of organizations have mobile employees.[1]

1/5 of smartphone users use their phone for most of their online browsing.[1]

Case 1: Large Technology Company

Background: The company is a large technology provider located in Europe. It has offices in multiple countries, including the U.S. While software developers typically work from the office, other staff such as sales engineers, business development staff, and executives are highly mobile. Even though the company processes a relatively low volume of Personally Identifiable Information (PII), it has a significant portfolio of Intellectual Property (IP) to protect.

Visual Privacy Strategy: This company takes a risk-based approach to Visual Privacy and stratifies employees by level, access to IP, and frequency of travel. Most executives and frequent travelers (including legal staff, engineers which work with other groups/ locales, sales engineers, etc.) are given screen privacy filters for their laptops and are required by policy to use them while working outside of the office. The company goes a step further by not allowing some employees, through policy, to work on their laptops on airplanes. When using a visual privacy filter, most employees are permitted to work in other public locations.

Privacy is
the best policy.

3M

Case 2: Large Manufacturer

Background: The company is a large manufacturer that builds hardware for the U.S. government as well as corporations. The company is highly segmented — business units run with near autonomy, and policies and practices are largely set within those business units with a few policies inherited from corporate. This segmentation stems from the fact that some of the business units are working on government contracts where they are required to follow a specific set of standards. Some of these business units have their own security officer, and there is also a security group which sits outside of the business units and serves in an advisory capacity.

Visual Privacy Strategy: Overall, the company makes screen privacy filters a "request item." Employees can request a filter, and if approved by their manager, one will be supplied. Within certain business units however — primarily those working on government contracts — screen filters are required on laptops for the entire engineering staff. In these business units, filters are issued with new laptop purchases or when a laptop is provisioned. A policy exists on limiting work in public places for these engineers. At a corporate level, screen privacy filters are provided to executives, recommended by the Chief Security Officer, but their use is not enforced.

Case 3: Regional Bank

Background: The company is a regional Midwest bank with multiple branches. The company processes a significant volume of legally protected data such as PII (name, social security number, etc. of its customers) and also payment card information. As a result, the company's information security strategy is largely driven by regulation and industry standard, the most impactful of which has been the Payment Card Industry Data Security Standard (PCI DSS). Additionally, the company is located in a state that has a breach notification law, requiring the bank to inform customers if they believe their data has been exposed. More broadly, the bank has customers that are legal residents of many other states and thus they fall under multiple state breach notification laws.

Visual Privacy Strategy: The company has no explicit policy on when work is permitted outside of the office and what security controls are required — typical of a company this size. In practice, most bank executives use screen privacy filters. Several of these executives frequently travel regionally, as well as occasional travel to the East and West coasts of the U.S. Within the bank branches, screen privacy filters are used on all teller monitors. Bank branches are typically configured with a row of tellers on one side facing customers, and then a drive-up service behind them. This leaves screens potentially exposed to other customers at the bank and was the primary driver for the adoption of screen privacy filters.

Conclusion

These three scenarios are a sampling of corporate strategies around visual privacy. Defending an enterprise from a data breach requires a combination of technical, policy, physical and people controls. The defense of data in-use is an under-addressed but increasingly important area. This need has been accelerated by the explosion of mobile devices and the move to cloud-based solutions where data can be accessed any time, anywhere.

The key to a successful visual privacy strategy is understanding risk, which is a function of both sensitivity of data processed and frequency of work in exposed areas. Particularly at risk are workers that have high mobility and access to sensitive data such as field technicians, field medical workers, legal, HR, flex workers (employees that regularly work outside the office), marketing staff, and engineers.

Screen privacy filters are important security controls to protect data from unauthorized insiders as well as external observers. They effectively block out side views and can help enterprises reduce the risk of exposing sensitive data. 3M™ Privacy Filters lead the industry and come in a range of sizes and styles to protect laptops, desktops and even mobile phones.

For more information visit: **http://www.3Mscreens.com.**

3Mscreens.com

[1] Privacy and Data Management on Mobile Devices, http://www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/

**Privacy is
the best policy.**

3M