Three High-Risk Employees Compromising Company Security

Defending an enterprise from a data breach (both malicious and accidental) requires a combination of technical, policy, physical and people controls. With the rise in worker mobility, organizations have been forced to re-examine their data security strategy. One important and under-addressed area is visual privacy — the protection of data as it is displayed on a screen. The explosion of mobile devices and the move to cloud-based solutions where data can be accessed any time, anywhere, means that more screens will be displaying sensitive data — often in public places like coffee shops and airplanes. Applying a risk-based approach to enterprise visual privacy protection is critical to any data security strategy. This paper outlines an approach to stratify employees and apply the proper tools, policies and education to reduce the risk of a visual data breach.

Separating employees into risk groups can help when building an operational strategy around visual privacy. The key is understanding which groups access and display sensitive information and how often they work outside the trusted confines of the office. Key groups to consider include:

Executives: Executives typically don't access customer social security numbers or payment card numbers, but the information they do access can have much greater visual breach consequences. Documents that talk about future non-public plans of the organization, the health of the business (including corporate financials), and sensitive corporate information including human resource issues, mergers and acquisition information, and trade secrets can have serious consequences when exposed. This information is particularly at risk when editing or viewing artifacts like PowerPoint slide decks given that PowerPoint content is usually created to be read at a distance.

Finance: The finance group processes particularly sensitive information within a corporation. If exposed, this data can have serious organizational implications, such as triggering Securities and Exchange Commission (SEC) violations. The risk is particularly severe for publicly traded companies where pre-release financial data can be used to make trades.

Sales: While sales collateral may not be considered sensitive or confidential, customer lists, which may include highly regulated data like social security numbers and credit card numbers, prospect lists, pending deals, and sales figures can be some of the most sensitive information that the organization maintains. Corporate sales staffs are usually highly mobile, working often on planes and in airports and coffee shops more than in their actual offices. The sales staff needs to be sensitized to the risk of a visual data breach through education.

It is important for security officials inside each organization to take a hard look at the groups and individuals who routinely work outside of the office, and exactly what type of data they have access to, in order to get an accurate picture of the risk of a visual data breach. Risk is a function of both sensitivity of data processed and frequency of work outside the office. Beyond the groups discussed above, field technicians, field medical workers, legal, HR, flex workers (employees that regularly work outside the office), marketing staff, and engineers can pose significant risk depending on their work patterns and data accessibility.

Adding privacy filters is a critical security control in protecting data from unauthorized insiders as well as external observers. The Visual Data Breach Risk Assessment Study – a study performed by People Security and commissioned by 3M, the makers of privacy filters – indicates that equipping at-risk employees with tools such as privacy filters must be coupled with policy to be effective. During a survey of 800 working professionals,two-thirds (67%) of respondents indicated that they view sensitive data outside of the workplace, including regulated and confidential information. By blocking outside views, privacy filters can help reduce the risk of sensitive data exposure.

The key is to educate any at-risk employees through educational modules, providing them with the proper tools to protect sensitive information such as timed screen blackouts or privacy filters, as well as setting policies that regulate when sensitive data can be accessed and enforcing the use of those tools.

46%

of cloud users say a major reason they used cloud apps is because they like being able to access their data from wherever they are or whatever computer they're using.[1]

Find out more at 3M.ca/SecureMyScreen

[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