3M Addresses Need for Stronger Visual Privacy in Healthcare and Finance

Safeguards beyond physical and cyber security are required to help protect data in high-risk industries

Organizations are investing in information security at record levels yet remain vulnerable to low-tech threats such as visual hacking, where someone can capture sensitive information with nothing more than a smartphone camera. In response, 3M has launched its Visual Hacking Key Risk Areas educational campaign to help security professionals and IT managers in high-risk industries better understand where vulnerabilities to data privacy exist and how they can be secured.

Worldwide spending on information security will reach $75.4 billion in 2015, an increase of 4.7 percent over 2014, according to the latest forecast from Gartner, Inc.[1] but such investments might not address all areas where data vulnerabilities exist. Ponemon Institute recently conducted the Visual Hacking Experiment, jointly sponsored by 3M Company and the Visual Privacy Advisory Council, on visual hacking, defined as the viewing or capturing of private, sensitive or confidential information on a screen device, workspace, copier, etc. for unauthorized use. It found that a white hat hacker was able to gain access to participating companies and visually hack sensitive information in 88 percent of attempts.

“Visual hacking can target any industry but may be especially dangerous in healthcare and financial industries, given the sensitive information involved in nearly every customer interaction and the desire for malicious parties to obtain it,” said John Brenberg, Information Security & Compliance Manager, 3M and member of the Visual Privacy Advisory Council (VPAC). “The 3M Key Risk Areas campaign aims to help these organizations understand the threats that visual hacking poses and help them expand their privacy programs to include much needed administrative privacy measures.”

Privacy key risk areas that visual hackers may target in these high-risk industries include:

Financial Services

Lobbies and public areas
Teller desks
Platform desks
Printers, copiers and fax machines
Drive-up teller windows
Shared / open workstations

“Data is the lifeblood of today’s digital businesses. Protecting it from theft, misuse, and abuse is the top responsibility of every security and risk leader,” stated a report by Forrester Research. “Hacked customer data can erase millions in profits, stolen intellectual property can erase competitive advantage, and unnecessary privacy abuses can bring unwanted scrutiny and fines from regulators while inflicting reputational damage.”[2]

A 2015 report by Forrester Research recommends verifying and securing all resources, regardless of location. This could entail using applications to mask high-risk data or privacy filters to shield data from onlookers, to name a few. Revising company policies to ensure workspace designs and employee behaviors are in line with data privacy best practices is another consideration.

To download the new educational resources, visit www.3mscreens.com/visualhacking.

About 3M

At 3M, we apply science in collaborative ways to improve lives daily. With $32 billion in sales, our 90,000 employees connect with customers all around the world. Learn more about 3M's creative solutions to the world's problems at www.3M.com or on Twitter @3M or @3MNewsroom.

[1] "Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015", Gartner, Inc., September 23, 2015
[2] "The Future Of Data Security And Privacy: Growth And Competitive Differentiation", Forrester Research, Inc., July 10, 2015

3MJane Kovacs, 512-984-67473M Media RelationsorPadillaCRTClaire Woit, 612-455-1735claire.woit@padillacrt.com

---

https://news.3m.com/2015-12-16-3M-Addresses-Need-for-Stronger-Visual-Privacy-in-Healthcare-and-Finance