Published on *The National Law Review* https://natlawreview.com

Data Breach Risk: What's Next?

Article By:

Paul Paray

Ten years ago, many companies didn't even ask about using encryption to protect data. Over the years, that has changed. More security and privacy professionals began to see it as an option in their cybersecurity defense. Then it eventually became a necessary component of most companies' security strategies and the use of encrypted laptops became a condition precedent for many cyber and privacy insurance policies.

Now, after strengthening their cybersecurity with encryption and other measures, companies need to identify the next potential data exposure points where bad actors can likely turn their attention. One overlooked vulnerability is the visual display of sensitive data on screens.

Protect Visual Privacy

Not every risk management, security and IT professional is familiar with visual hacking, but they should be.

Visual hacking is the unauthorized capturing of sensitive, private or confidential information for unauthorized use. It can include visually stealing information from someone's phone screen, viewing information left on a printer at work or other opportunities of information that is in plain sight. Very likely, it is already happening to workers in your organization.

It is commonplace for professionals who travel for work to access sensitive corporate material on the go. They could be riding on a train, plane or bus and simply open their laptops, giving those seated next to them full view of their work. In these situations, no one can be certain they are not exposing sensitive information—even something simple like a network username. It is not likely such a road warrior can be aware at all times whether another person is viewing or capturing what's on their screen.

A study conducted by the Ponemon Institute revealed that 87% of mobile workers have caught someone looking over their shoulder at their laptop in a public space. Yet, despite this potential risk, more than half of mobile workers surveyed said they took no steps to protect important information while working in public.

Visual privacy risks don't just exist outside the office. A worker who steps away from his or her

computer or has a screen facing a public walkway can also expose highly sensitive data to onlookers.

Reduce Your Risk

As with any risk, companies should evaluate the severity and potential frequency of visual privacy exposures to better understand their risk. An insurance broker can help determine if insurance coverage is available for these risks or if insurance premium credits may be available for implementing additional safeguards.

There are other steps any organization can take to reduce the risk of visual hacking. Working with IT departments and information-security officers, companies can implement small, easy changes to existing policies and procedures.

For example, companies can deploy privacy filters on laptops or mobile devices that darken screen data when viewed by onlookers from the side. These filters can also be fitted on device screens in an office to help limit the views of potential insider threats. For example, a receptionist should likely have such a privacy screen in place if his or her screen can be viewed by visitors.

Clean-desk policies should also be in place. Such a policy can reduce the display of sensitive information in printed and electronic forms when workers are away from their desks. Workers should also be printing or storing sensitive information in locked areas and use crosscut shredders to destroy sensitive material.

Finally, because visual privacy can only exist if workers adhere to policies, training is obviously important. Workers should be trained on the importance of visual privacy and being aware of their surroundings. They should also receive regular training on an organization’s privacy policies and associated safeguards.

Tackle Uncertainty with Certainty

Visual privacy may seem like an additional, unnecessary risk management burden to bear. But, like any other potential threat to sensitive data, it deserves attention. After all, a visual hack can leave no trace of when, where or how it happened—and such uncertainties may become problematic when addressing a data breach.

National Law Review, Volumess VIII, Number 205