HUMAN ERROR CALLED THE MOST COMMON FACTOR IN DATA BREACHES

Insights
12.14.15

As reported in the December 9, 2015 Wall Street Journal Law Blog, a recent report by the Association of Corporate Counsel ("ACC") revealed that the most common reason for a data breach at companies is "employee error."According to the report, which contained survey responses from over 1,000 in-house attorneys in 30 countries, 30% of the breaches this year resulted from employee error.Of course, this is not new news, but rather the most recent confirmation of earlier studies.For example, IBM's "2014 Cyber Security Intelligence Index" found that 95% of all security incidents involve at least some level of human error, whether intentional or unintentional.Other studies have estimated that as many as 75% of security breaches were "inside jobs."

Extreme cases can involve intentional conduct, like where an employee downloads sensitive company onto a thumb drive and walks out the door.But most security breaches by insiders are not intentional and cybercriminals are constantly changing their approaches to take advantage of employees.Other reports have concluded that these hackers even incorporate social engineering into their schemes to maximize the chances of successfully preying on an unsuspecting employee.Examples of employee conduct contributing to a breach include inadvertently responding to spam phishing emails, employees who interface between company and personal systems that may not have security in place, or employees working remotely on unsecure Wi-Fi networks.

Despite the fact that employee error is such a consistent factor, employers have seemingly been focused on other methods of protection.The ACC report indicated that although 56% of the respondents indicated that their companies are allocating more money to promote cybersecurity prevention, fewer than half reported that mandatory training exists at their companies.Even fewer indicated that their company tracks or tests employee knowledge.According to recent survey by CompTIA, "the main reason that companies exhibit a low level of concern over human error is that it is a problem without an obvious solution.""A high level of concern over malware or hacking can be addressed with an investment in technology," but human error can only be addressed through training, the success of which can be difficult to measure.

Not surprisingly, vendors are increasingly offering legitimate software options designed to minimize the human threat.For example, some offer security software that monitors sensitive information being leaked out of the organization and also monitors other prohibited employee actions like sending sensitive documents to a personal email or placing them on file-sharing sites or removable media like a thumb drive.While these are viable options, the first line of defense remains employee media like a thumb drive.While these are viable options, the first line of defense remains employee awareness.Employees still need to be initially trained and regularly updated to ensure that they understand the threats they face and the part they are expected to play in protecting against them.

Related People

Joshua H. Viau
Co-Regional Managing Partner
404.240.4269
Email