The Source of the Equifax Breach

Equifax has finally informed the public about the source of the dramatic data breach that occurred in July 2017 and was disclosed earlier this week. As is so often the case, a weak leak in the chain of information transmission caused this disclosure of confidential personally-identifiable consumer financial information.

> One of the key lapses in security at Equifax was due to the failure of its IT personnel to install a simple patch to the software that drives the Equifax e-portal for many months after its release.

Most websites deploy an open source application known as Apache to run their websites, e-commerce sites and interfaces. In March 2017, the Apache Software Foundation discovered a major vulnerability in its software code and that hackers were taking advantage of the security hole to steal information. Apache distributed a free software update to its customers to patch the security vulnerability. Most major corporations including Microsoft and others promptly installed the patch and averted disaster. For unknown reasons, the IT staff at Equifax did not install the patch for 2-½ months. This extreme delay permitted rogue actors to obtain data dumps of 143 million consumer records. Equifax reportedly first became aware of the incident on July 29, while the breach is believed to have occurred from mid-May through July.

I do not know if the bad actors who committed the breach were outside hackers, or employees with malevolent intent, or if the failure to install was due to employee ignorance, sloppy work habits, or laziness. In any event, the hole remained wide open for hackers, sovereign nations. computer-oriented teenagers, and others to exploit. And the worst outcome occurred. The security vulnerability could have remained open without being hacked. Unfortunately for Equifax, the opening was attacked and breached, disclosing a fountain of information outside the protective umbrella of Equifax's data centers.

> One of the many lessons to be learned from this tragic incident is the need for preparedness and planning before a cyber event occurs. Planning advance is no longer optional. Considering the future is no longer best practice. Strategic planning to protect an enterprise's computing environment is as mission-critical today as is keeping the business' bank accounts reconciled.

Cyber liability insurance, breach notification, insider trading, credit freezes, criminal charges may all be in Equifax's future. For certain, the value of its brand and goodwill have been tarnished forever. But for purposes of this article, a key lesson learned from this cyber incident is the need for every business to plan and to coordinate efforts among IT staff and the C-suite because after all, the buck stops with the CEO and the board of directors.

Be prepared.

Associated Url: The Source of the Equifax Breach