Employees are a huge security problem, but IT built the monster themselves, SailPoint survey says

March 22, 2016 | Written by Alyssa Huntley and originally published on FierceCIO.com

The biggest threat to a company's digital security seems to be its employees, according to the 2016 Market Pulse Survey, sponsored by SailPoint Technologies [reg. req.]. But before the finger pointing gets underway, it appears IT departments built that monster themselves.

One third of respondents said they share their passwords with their coworkers, and nearly two thirds (65 percent) said they only use a single password across multiple applications.

Yet, the most terrifying revelation is that one in five employees globally said they would sell their passwords to an outsider. While 44 percent would sell credentials for less than $1000, some would even sell them for less than $100.
The study broke down that 20 percent who would sell passwords by country. The U.S. led the pack with 27 percent willing to sell.

These numbers seem odd, given the information on how personal attacks have become, and how concerned workers are. When it comes to personal information, 32 percent of respondents said they have been impacted by recent data breaches. A whopping 84 percent expressed concern about personal information being shared by corporations they do business with.

Employees have legitimate reason for concern. A survey from security firm Sophos found that many companies fail to encrypt sensitive employee data. "Sensitive employee information, including banking details, human resource files and health care records, is not being encrypted by many midsized businesses surveyed by network and endpoint security firm Sophos," a FierceITSecurity article noted. "The security firm polled 1,700 IT decision makers from midsized businesses in the United States, Canada, India, Australia, Japan and Malaysia. It found that 31 percent of respondents said they do not always encrypt employee banking information, 43 percent do not always encrypt sensitive HR files, and almost half do not always encrypt employee health care information."

Companies should be concerned about these numbers, as well. A majority of respondents (85 percent) to the SailPoint survey said they would react to a company that experiences a data breach, which could include cutting off ties with it.

It seems as though IT has quite a rogue group to worry about. It also seems as though IT may be to blame there. The survey showed that, when it came to purchasing apps to

use at work, almost half of respondents (49 percent) would circumvent IT "because it was faster," 40 percent because "IT adds too much process," and 21 percent because "IT over complicates things."

It isn't just current employees that IT should be concerned with either. When it came to folks who left a company, 42 percent were able to access old accounts or data after termination. It seems as though IT teams leave more than a few doors open to non-employees.

"The digital identity of an individual user is the key that unlocks corporate data and applications…" The survey said. "Organizations need to strike a balance between providing the level of convenience the employees require (and expect) while also ensuring that proper IT and security controls are in place. Corporate security and business agility can no longer be competing priorities, but instead must be interwoven."