Inattentive employees pose major insider threat

By Fahmida Rashid, ThirdCertainty

When it comes to insider IT security threats, the biggest exposure companies face isn't from vengeful or disgruntled employees. It's from the inattentive ones.

Some 80 percent of network data breaches are accidental, according to a recent customer survey conducted by endpoint security vendor CoSoSys.

Infographic: *Assessing insider threats*

CoSoSys found that over half of employees have accidentally sent emails to the wrong person and 59 percent think losing a mobile device or laptop with company data isn't "too big" a threat. That's a lot of lost devices potentially not reported to IT.

"Breaches caused by negligence, human error and lack of proper training are more common than breaches caused by malicious insiders," says Roman Foeckl, CEO of endpoint security company CoSoSys.

Diverse damage

A data breach has serious financial implications, both directly and indirectly. A recent Ponemon Institute survey pegged the cost of a data breach, on average, at a whopping $3.5 million.

The direct costs are easy to calculate: the cost of special investigators hired to track down the incident, the time and resources spent to remediate the issue, and lost revenue and productivity resulting from company downtime. The indirect costs are less obvious, such as brand damage and loss of consumer trust.

"In addition to any fines a company has to pay in association with a breach, there is a huge amount of lost revenue that will not be coming in," says Foeckl.

A look at the biggest security headlines from the past year—Target, Home Depot, P.F. Chang's, Sony—might suggest the biggest threats for organizations come from outside adversaries. But for every Target, there is a Morgan Stanley, where an employee was behind the data breach. In fact, insiders pose a more immediate threat to most organizations.

An organization can be breached because passwords to sensitive systems were shared freely or because confidential files were not adequately protected. Malicious outsiders can also take advantage of weak passwords and mis-configured systems to impersonate an authorized user on the network. Target can be considered an insider attack since the attackers pretended to be from the retailer's HVAC provider.

Range of risks

Employees need to understand the full range of ways sensitive company information can end up in the wrong hands, regardless of the exit point, such as USB storage devices, file sharing applications, cloud storage, social media, emails, messengers, other online applications and even printers.

Breaches by malicious insiders tend to receive the most attention because they have the potential to cause more damage. Consider the kind of sensitive information key employees have access to and it's clear the repercussions to the business are "exponentially higher than a human error incident," Foeckl says.

Employees aren't being malicious or negligent—many of them don't realize that security is part of their job description. When 35 percent of employees say data security is not their responsibility, organizations need to pay attention. The IT department has to put the proper tools in place to prevent and detect data breaches, but employees also have to be educated regularly on the steps they need to take to avoid a potential breach, Foeckl says.

Focusing all efforts on keeping the bad guys out means organizations are caught off guard when the threat is already inside. Spend a portion of the budget to deal with insider threats by implementing systems to grant access only to the extent employees need to perform their jobs. It's a challenge to implement security without severely impacting day-to-day activities, but it will be far cheaper than the final cost of the data breach.