Corporate Network Snooping: Employee Behaviour Exposed! And the Solution!

A recent One Identity survey of 913 individuals revealing shocking statistics regarding employee snooping on corporate networks. The results are unnerving because the number of employees across countries and sectors is very large, and majority of the respondents admit to doing some snooping themselves. Snooping is defined as gaining or attempting to gain access to data that does not pertain to the job. It seems Identity and Access Management has a bigger role to play in anti-snooping from within the corporate network than previously thought. Here's the lowdown.

While the survey respondents constituted primarily of individuals from the USA (34%), respondents from other regions are represented well enough (Hong Kong: 11%, Singapore: 11%, Australia: 11%, France: 11%, Germany: 11% and United Kingdom: 11%). The survey therefore represents each regional sample appropriately enough for accurate results. All company sizes were accurately represented as well, with 500-2000 employees at (44%), 2000-5000 at (28%), and more than 5000 employees at (28%).

Of those surveyed, majority were team managers (45%), which ensured that relevant people in the organization who are in a position to observe employee behaviour made up the meat of the sample. Executives were also represented at (35%) and 'individual contributors' were at (20%).

The individuals also, by a majority, already had privileged account access (87%), which makes it even more alarming that they still felt the need to snoop the corporate network for more data. Or, perhaps having access to privileged data gave them a taste and they wanted more. Whatever the case, this represents a scenario where employees were not starved of access to data, but still felt the need to snoop some more. This uncovers behavioural trends towards snooping that are psychological in nature, and therefore must be addressed at the security level rather than in any other way.

When asked the question, "In your experience, do EMPLOYEES ever attempt to access information that is not necessary for their day-to-day work?", 69% said "Rarely, but it happens", 23% said "Yes, this happens frequently", and only 8% said "No, they never even try."
This places 92% of employees in the 'potential insider threats' category, which is a whopping percentage. When asked instead the question, "Have YOU ever attempted to access information that is not necessary for your day-to-day work", the numbers again favored snooping. (51%) responded "Rarely, but I have done it" and (15%) replied "Yes, I do this frequently".

And critical performance data is regularly being compromised as well. More than 1 in 3 (36%) respondents replied 'Yes' to the question "Have you ever looked for or accessed sensitive information about your company's performance, apart from what you are required to do as part of your job?" Such statistics could spell disaster for all sizes of businesses. Data breaches are expensive, but performance related breaches moreso. These can threaten the very survival of your business.

The situation clearly demands attention. How can one reduce the threat of insider snooping?

Identity and Access Management (IAM) has the answer. Role-based access control and strict governance of rights and permissions can help prevent potential bad actors from accessing confidential or sensitive information. With regard to snooping done by IT security professionals specifically, organizations can leverage identity intelligence to identify who has elevated rights and help pinpoint exactly where abuse of those rights is occurring.

Ilantus Compact Identity offers a single solution that allows role-based access control, governance, and risk metrics powered technology to identity privileged accounts. The solution also is the industry's first to offer Single Sign-on, Enterprise Class Password Management, access recertification, and in fact all essential IAM components that most businesses require to secure themselves against insider threats. The solution is also the most economical on the market, and requires a single purchase for both Access Management and Identity Governance features. Most other products offer only one or the other, which increases complexity and cost. It can also be acquired as a perpetual license, subscription, or on a pay-as-you-consume basis, which is also an industry first.

The solution was built from the ground up to solve REAL customer challenges. Other vendors provide 'one-size-fits-all' solutions and try to place 'square pegs in round holes'. They also innovate only to provide the best-selling features, and not to solve existing customer challenges. For instance, Ilantus offers the world's only 'thick-client Single Sign-on' possibility, which is a common challenge among customers. Other vendors might offer the latest technologies available in the domain, such as adaptive authentication, but miss out on foundational features. The reason is that **they engineer what sells**, rather than **what's needed**.

Ilantus does not make this mistake. Check out Compact Identity today!