Insider Threat and Personnel Security Case Study

By: Gerald Rigdon - 2023

How does personnel security relate to the security of information systems?

Personnel security along with information security and physical security (*Importance of Personnel Security*, 2023) have been described as a three-pillar security system. The relationship between personnel and information security is particularly pronounced given employees or ex-employees are often the weakest link in a security chain. While physical security should always be a concern, information is more likely to be targeted by company personnel. Hence, a vibrant security culture requires proper screening of potential job hires including background checks and effective job interviews and training programs once employed. The benefits reaped include engaged employees, better compliance, reduced insider incidents, security threat awareness and people who are more security-conscious (*People Risks for Users*, 2023). Further, susceptibility to security vulnerabilities may be increased by:

- Ineffective leadership governance structures
- Inadequate personnel security policies, procedures, and screening
- Poor management practices that reduce trust
- Ineffective training during onboarding and ongoing
- Lack of a strong security culture

People can be both the biggest asset and liability. Having effective personnel security ultimately mitigates the risk of insider information security breaches.

What are some of the reasons companies continue to, unintentionally or otherwise, have ex-employees maintain access to sensitive systems?

In a study that included 379 online surveys (*Do Ex-Employees Still Have Access to Your Corporate Data*, 2014), the research found that 60% of employers did not request cloud application login credentials from former employees. It also concluded that much of the problem centered around employees owning the devices that were granted access. The Bring Your Own Device or BYOD phenomenon has far-reaching consequences, from medical device companies allowing access to implantable devices from applications running on phones owned by patients, to employers allowing an entire range of corporate tasks to be performed on property owned by the employee. Hence, in many organizations, it is not clear who owns the process of ensuring the decommissioning of ex-employee access.

Also, (Dontov, 2020) suggests the primary failing occurs in the employee offboarding process which should include the following:

- An exit interview
- Prevention of email forwarding and file sharing
- Revoking access to all applications and services
- Resetting shared passwords
- Reassigning licenses to other employees
- Ending employment on a good note

How can the organizations ensure that their employees, especially the ones who were terminated through involuntary separation, will not misuse access to sensitive data such as credit card information, health records, intellectual property, etc.?

In the Medghyne Calonge case (Rayome, A., 2017), she began deleting data before she was escorted out of the building and for days afterward. As for Juliana Barile, she was a remote part-time employee who maintained remote access after termination even though an internal company request had been made to disable her access. Although it may be impossible to prevent misuse access, there are mitigations (*Importance of Personnel Security*, 2023) that can be put in place by employers as follows:

A. Employee Agreements

Employee agreements can help prevent future disputes by documenting the actions to be taken and governance rules in termination situations. While ex-employees should "know better," sometimes the legal consequences are not taken into consideration in the heat of the aftermath of termination. However, enforcing this early on by signed mutual agreements would serve as a deterrent.

B. Policy Reviews

New hires should be made aware of employment policies including employee handbooks and any other company documentation. This should include written acknowledgement from the new employee.

C. Training Programs

Training programs help reinforce good cybersecurity practices that once ingrained should continue post-employment termination.

What recommendations or additional thoughts can be provided regarding the mitigation or control of insider threats?

Although the assignment reading was focused on ex-employees, I argue just as much attention should be given to current employees. What I found interesting from one study (Posey, C. and Shoss, M., 2022) was that many cybersecurity violations are driven by stress rather than the desire to do intentional harm. After surveying 330 remote employees

across a large swath of industry, 67% reported failing to fully comply with security policies at a 1 in 20 occurrence rate.

It is often emphasized that effective company cybersecurity isn't possible without the complete support and funding from executive management. Therefore, when considering the cost of cybersecurity programs, one must think beyond the conventional assets associated with such programs and appreciate the hidden costs associated with employee compliance in the everyday job task workflow. Referring once again to the findings in (Posey, C. and Shoss, M., 2022) the stress related violations of security policies were attributed to the following reasons in 85% of the cases:

- Necessity for accomplishing job tasks
- Getting something that was needed
- To help others get their work done

Moreover, malicious intent accounted for only 3% of the policy breaches, which boils down to non-malicious breaches occurring 28 times more often. The conclusion reached was: "People were more likely to violate procedures when they worried that following them would hinder productivity, require extra time or energy, mean doing their jobs in a different way, or make them feel like they were constantly being monitored."

Therefore, a healthy security culture means executive management must recognize and continually message to the workforce that no one should ever feel pressure to violate company security policy to get their job done. The overhead of security policy compliance must be factored into the creation of realistic project schedules and milestones.

References

Do Ex-Employees Still Have Access to Your Corporate Data? (2014, August). Osterman Research Group. intermedia.com. https://www.intermedia.com/assets/pdf/do_ex-employees_still_have_access_to_your_corporate_data.pdfLinks to an external site.

Dontov, D. (2020, August). *The Cybersecurity Risks Of Improper Employee Offboarding.* forbes.com. https://www.forbes.com/sites/theyec/2020/08/04/the-cybersecurity-risks-of-improper-employee-offboarding/?sh=74be635a1bfeLinks to an external site.

Importance of Personnel Security (2023, April). ivypanda.com. https://ivypanda.com/essays/personnel-security/Links to an external site.

People Risks for Users (2023, February). npsa.gov. https://www.npsa.gov.uk/people-risks-usersLinks to an external site.

Posey, C. and Shoss, M. (2022, January). *Research: Why Employees Violate Cybersecurity Policies*. hbr.org. https://hbr.org/2022/01/research-why-employees-violate-cybersecurity-policiesLinks to an external site.

Rayome, A. (2017, August). *Why ex-employees may be your company's biggest cyber threat*. techrepublic.com. https://www.techrepublic.com/article/why-ex-employees-may-be-your-companys-biggest-cyberthreat/