Trent

Ch 12 Access Management

7/31/18

12-3 Best Practices for access control

Most people want to trust their coworkers are working for the good of the organization but is more like a Russian Doll with many layers. For some it is for the money and satisfaction of doing good, while for a few are tangled into a mess from one wrong action into a life of crime. Whatever the reason for becoming a Russian doll at the organization can bring criminal charges once caught.

One idea is to separate job duties to reduce the risk of Russian Dolls. One example is at Countrywide financial where two co-workers partnered to sell data to other brokers. One stole the customers data, and the other claimed it was sales leads to other mortgage brokers. The company did prevent USB ports, but one computer had a flaw to allow coping in the office. Sold 20,000 customers complete data each week for 2 years and made around $50,000 to $70,000 (2006-2008) (Mullins, 2008). The problem with separation is that coworkers become friends and may plan on making some side money since the organization will not notice at all. One solution is to separate the different department groups by floor, section, or building to prevent different people from overusing their power.

Another idea is job rotation and can reduce the risk of Russian Dolls. Job rotation problems happen mostly from outsourcing and not having the current employees working on a project. It happened to NASA in September 1999 with Mars Climate Orbiter with the teams not coordinating on using Metric or English measurements, and caused the $327 Million Dollar disaster from the ground at NASA using American, and the space craft using Metric on the failed burning descent from the different measurements (nariski, 2013). Even though job rotation can stop corruption but will cause very different ideas on how to handle the systems.

A different idea to stop Russian Dolls is mandatory vacations after so many days. One example is from New York state employee who got entangled into a money scheme by cashing a $100 check to help pay for 6 kids, and a sick wife while living on a state salary. The vendor threatened to report the bribing if the worker did not do what was told and stretched beyond allowed duties to buy items for the state costing a total of $350,000 all to sub-companies of the briber that was generous to give 10% kickback. The only reason caught was forced to take a vacation to care for his wife after being at the office each day for 3 years, and the only reason was three odd locking invoices sent to the office that were not in the files (Wells, 2004). It could just be me, but I don’t cash unknown money or open up an email saying I won money. The best solution would to have come clean with the boss, and that it would not happen again.

The last solution is to have a clean desk. In 2006 17.5 Million Military Veterans and personnel names, birthdates, and social security numbers stolen from a laptop a VA employee took home without permission (nariski, 2013). This one is not the easiest for some, and my dad has a clean desk at his office if he is allowed to have 11x17 paper stacks as the surface. It is not always possible to move paper organized stacks, or ability to leave the laptop while going on a business trip. The main thing is to put confidential items in a locked cabinet, and logout of the computer.

Overall some layering of all four is needed. The most important one is mandatory vacations to avoid corruption and burn out of employees. The next most important is separation of duties to avoid collusion to affect the outcome of the organization. Clean desk is one that should be limited, but with caution. The reason is that computers are needed for business trips, so the best solution is teaching employees how to be smart while out of the office with the computer and paper. The last one of job rotation should not happen because it would lead to employees not knowing what they are doing and feel lost. Breaches of security are going to happen anyway so making employees suffer with rules that are not needed but is more teaching them to look out for certain behaviors in coworkers and on business trips of someone wanting to access the data.

# References

Mullins, R. (2008, November). *Lessons learned: The Countrywide Finacial Breach.* Retrieved from SearchFinacialSecurity: https://searchfinancialsecurity.techtarget.com/tip/Lessons-learned-The-Countrywide-Financial-breach

nariski, S. (2013, April 10). *Th 25 costliest teck screw-ups of all time.* Retrieved from it manager daily: http://www.itmanagerdaily.com/the-25-costliest-tech-screw-ups-of-all-time/

Wells, J. T. (2004, April 30). *The Case of Pilfering Purchase Manager.* Retrieved from Journal of Accountancy: https://www.journalofaccountancy.com/issues/2004/may/thecaseofthepilferingpurchasemanager.html