Tyler Poor

Professor Henderson

CSCI 325

8 June 2020

Problematic Internal Issues: The Effect in the Corporate World

In modern day society, most corporations are pushing to be more advanced than all others. The need for these advancements can help businesses to grow exponentially more than their competition. The key to this growth is information. Information allows for competitive business insight, gaging customers, future predictions, financial help, and many other avenues of corporate breakthrough. However, since information holds such great value in today's society, the enticement to steal such information is ever-present as well. This idea goes against all ethics, not only societally and morally, but also biblically.

Information can be used in a both beneficial and unbeneficial manner. Therefore, the need to protect information is growing throughout technologically advanced countries. In the realm of information security, the ideas of confidentiality, integrity, and availability (CIA triad) are prevalent and used often when evaluating a piece of information. In an academic journal, Warren Axelrod states, "For any given piece of data we must ask: Is it protected from being disclosed to those who should not access it? Is it protected from being created, changed or deleted by those who do not have permission to do so? And, is it available to those who need it? (9). Therefore, with these values in mind, it is crucial for company employees to abide by these principles and find ways in which to stop others who are not doing so. The trickiest place to do this is within the confines of the company walls. Most people believe that different forms of technological threats such as, malware, adware, phishing, and rootkits hold the highest threat

level; however, the biggest threat to growing companies and novice workers is the internal threats of an unsuspected employee with proper authorization.

The ability to reasonably ensure conformity and adherence to both internal and external policies, standards, and procedures within a company, seems to be the biggest ethical mishap in the realm of information security. Personally, the value of information has been established to me through the words and explanations of others; however, this same mindset has not been established to all. In an academic journal, Allen Johnston states, "Information security policies present many technical solutions (e.g., email encryption and anti-virus) and procedural guidelines (e.g., lock computer and choose strong passwords), but it is widely reported that employees do not comply with the policies or deliberately bypass them"(246). As can be seen, regardless of the vast amount of technical solutions and security policies in place, it is ultimately given to the individual to decide whether or not they should follow them. Personally, these issues will be displayed in my future place of work; therefore, it is critical for me to be on guard about the theft of company information, and how I can be spiritually prepared for this. Unfortunately, because of sin, the human nature is one of deceit, deprivation, and defiance. Jesus himself makes this clear when he states, "But those things which proceed out of the mouth come from the heart, and they defile a man. For out of the heart proceed evil thoughts…thefts, false witness… These are the things which defile a man" (Matthew 15:18-20, New King James Version). Therefore, the enticements to benefit from the theft of information is alive and well and will be until information loses its value.

The ability for an employee to be tempted in misusing company information is ever present and growing throughout the years. The reason for this growth, is because of the amount of personal gain that humans continually seek for themselves. In a peer-reviewed article,

Amanda Chu states, “In addition, by definition, misbehavior in networks/applications involves the use of illegal software, which affects the privacy of information and is a common workplace problem. Employees engage in misbehavior in networks/applications mainly because they want to receive personal benefits such as time savings (16). Since this growth is so obvious, it is crucial for new workers to stay grounded spiritually and morally in the word of God, in order to find strength in the midst of a tempting environment. In doing so, they “will be able to quench all the fiery darts of the wicked one” (Ephesians 6:16, New King James Version) and “flee these things and pursue righteousness, godliness, faith, love, patience, gentleness” (1 Timothy 6:11, New King James Version). As a Christian going into a majority secular workforce, it is imperative for me to remember 1 John chapter four, verse four, “You are of God, little children, and have overcome them, because He who is in you is greater than he who is in the world” (New King James Version). Being led by the Holy Spirit in world of lust and temptations is the best way in which someone can handle these problems within a vastly growing technical field.

Ethical standards are to always be upheld, especially within the confines of personal company information. The indispensability of this information is what gives it its highest value. With that, it is integral that ethic codes such as in the ACM Code of Ethics and Professional Conduct, be adhered to. Ideals like “Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing”, “Avoid harm”, and “Be honest and trustworthy” should and will be followed by the employee who is grounded in biblical truth (ACM Code of Ethics and Professional Conduct, 5-14). If these codes are held by all employees within a company, it will be able to operate with the best ability possible. These moral ideologies come from a biblical worldview. In the book of Ephesians, it states, “Let the thief no longer steal, but rather let him labor, doing honest work with his own hands, so that he may have

something to share with anyone in need" (4:28, New King James Version). Also, in the book of first Timothy, it states, "For the love of money is a root of all kinds of evils" (1 Timothy 6:10, New King James Version). Now, since these foundational truths are set, it is essential that employees build themselves on these truths and encourage others within the company to do so as well. Holding each other accountable for following such moral standards is how the company can run without flaw. The temptation to steal will be evident and available to the employee with the proper credentials. However, if this employee is founded on biblical truths and ideals, seeks the face of the Lord daily, and is led by the Holy Spirit, they will be able to resist any temptation that comes their way.

In conclusion, the biggest ethical threat to face the growing technical field is the opportunity and risk for an employee to steal company information for personal gain. This, however, does not mean that they are entitled to do so. The possibility of this happening is up to the employee. Although this is true, if the employee is grounded upon biblical truths, they will be able to resist this temptation. For the Christian entering the secular workforce, these truths need to be embedded in them in order to work to the best of their ability and to push their co-workers to do this as well.

Works Cited

Axelrod, C.Warren, et al. *Enterprise Information Security and Privacy*. Artech House, Inc, 2009. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=e000xna&AN=285008&site=ehost-live.

Chu, Amanda M. Y., and Mike K. P. So. "Organizational Information Security Management for Sustainable Information Systems: An Unethical Employee Information Security Behavior Perspective." *Sustainability*, vol. 12, no. 8, MDPI AG, Apr. 2020, p. 3163–, doi:10.3390/su12083163.

Johnston, Allen C., et al. "Speak Their Language: Designing Effective Messages to Improve Employees' Information Security Decision Making." *Decision Sciences*, vol. 50, no. 2, Apr. 2019, pp. 245–284. *EBSCOhost*, doi:10.1111/deci.12328.

NKJV Study Bible, Third Edition. Ronald B. Allen, Thomas Nelson, 2018.

"The Code Affirms an Obligation of Computing Professionals to Use Their Skills for the Benefit of Society." *Code of Ethics*, www.acm.org/code-of-ethics#h-1.3-be-honest-and-trustworthy.