Securing Proprietary Information in Healthcare: Human Controls

Mansur Hasib, CISSP®, PMP®
Chief Information Officer
Baltimore City Health Department

Abstract

Securing proprietary information is a problem for all organizations. Historically there has been a higher reliance on technical controls to solve this problem. This paper examines the role of human behavioral controls and how these can be a highly cost effective and important in component of information security. The author elaborates how an organizational chief information officer in a healthcare setting can use human behavioral controls grounded around a set of core values to secure proprietary information used by self managed teams.

Technical Factors and Human Factors in Data Loss Prevention

One of the primary goals of any information assurance program is the security of proprietary information. This particular area can be broadly classified as data loss prevention. A comprehensive data loss prevention program will typically have technical controls and human behavioral controls. However, the data on security breaches show that the vast majority of data breaches happen through insiders; hence focus on insiders is central to many information security management programs. Insiders are defined as employees or affiliated and contractual personnel who have legitimate access to information (Probst, Hunker, Goleman & Bishop, 2010). In the healthcare industry, 80-90% of the data security breaches between 2008 and 2010 happened through insiders (HIMSS Analytics, 2010). Thus a focus on human behavioral controls by a healthcare chief information officer can have a major influence in guaranteeing the safety of proprietary information used by self-managed teams. Human behavioral controls are typically applied through policy, contracts, education and training, and through leadership and management techniques which promote an environment conducive to the security of proprietary information. Using materials from the author's leadership experience and Lussier and Achua's book *Leadership: Theory, Applications, & Skill Development* (2010), this paper suggests how an executive leader such as a chief information officer (CIO) in a large healthcare setting can use human behavioral controls, team development and other leadership and ethical concepts to secure proprietary information used by self-managed teams composed of physicians, nurses, and medical professionals/technicians. The typical controls such as data classification, authorization, encryption, data obfuscation, multi-factor authentication, auditing, monitoring, logging and other routine, physical and widely accepted information security layers are assumed to be present.

Values

In any organization, values are important because they define what the organization and its employees stand for. The CIO should work with his or her immediate leadership team as well as the senior healthcare leadership team to identify and agree upon a set of values that will be driven throughout the organization. These values can act as an internal barometer among all members of the self-managed teams as well as the rest of the organization. Everyone should know what the values are; they should know how to channel their behavior. These values would define the culture of the self-managed teams as well as the entire organization. Some powerful values that foster a secure and desirable behavioral culture are: integrity, empowerment, teamwork, customer service, continuous learning, and positive reinforcement. Integrity is a key foundation for an empowerment and self-managed-team-oriented culture. It allows someone to focus on doing the right thing at all times. Empowerment allows decisions to be made at the lowest level of the organization possible, thus allowing an organization to make more decisions and solve more problems at any given time. Teamwork creates a sense of interdependence and shared goals and shared success. It creates a sense of belonging, fosters allegiance and reduces staff turnover and churn. It can also make it fun and enjoyable for people to work in an environment. A customer service attitude ensures that the customer needs are addressed properly and the customer feels valued and has a higher probability of being retained. Customers who relish positive experiences will often ignore lower cost options simply for the pleasure and dignity of being treated right. Continuous learning ensures that the team will not stagnate and there is a spirit of constant adventure and innovation within the team. It also creates an environment for greater awareness of possible security threats. Positive reinforcement allows everyone to celebrate in the success of the team and its members. People who feel good about

coming to work will usually have higher levels of productivity. Empowerment, continuous learning and positive reinforcement allow everyone within the self-managed team and the organization to be engaged in its success. Thus the team and organization is run by the brains of all its members rather than the brains of a few anointed leaders.

Everyone should clearly know what the values of the organization mean and how they can be applied to their work within the self-managed teams and the organization. Recruitment into the organization, retention and rewards within the organization should be governed by the corporate culture and values. There should a method to deal with deviations from these values and everyone should clearly know and understand the consequences. Key values such as these are essential to the success of organizations because they promote morale, foster employee loyalty, improve productivity and result in higher retention rates. Though organizations have limits on their ability to compensate people financially, organizations and teams have unlimited amounts of non-financial rewards that they can distribute amongst themselves.

Policy and Contractual Controls

The CIO should adopt organization policies which clearly embrace the organizational values and identify appropriate use and safeguards of proprietary information. Each person who has access to such information should be required to acknowledge that they have read and understood the policy. Each person should be required to sign non-disclosure and non-compete agreements. These agreements should clearly require the non-disclosure and non-compete obligations to perpetuate perennially even after disassociation from the organization. There should be contracts with all related organizations with regard to mutual safety obligations related to proprietary information. It should be obvious to everyone that these documents and controls are extensions and instruments of the organizational values.

The data need to be classified in accordance with its sensitivity. There should be a conscious documentation of who needs access to what information and proper records need to be maintained on authorization of this access. There should be a proper change management process for changes to access controls. The teams should be fully aware of the sensitivity of the data they use and know who has access to what type of information. They should be vigilant in ensuring that everyone uses the information and access in a responsible and intended manner.

There should be policies and procedures to track when information is retrieved, by whom and when it is securely returned to its place of rest. Departures of any member should be governed by policies and procedures which remove access from people who are no longer within the team. Access could be time controlled as well as geographically restricted. Data could be prohibited from being moved, copied or carried away in an unauthorized manner. Controls and expenditures of resources need to be proportionate to the sensitivity and risk associated with the information.

Leaders Developing Leaders

Each layer of leadership should be trained on how to be a catalyst leader so that they can nurture and create other leaders and lead through adoption of organizational values. Everyone should have the ability and freedom to question unsafe actions by anyone. There should be a culture that promotes active confrontation and immediate correction of any unsafe action by any member of the organization. People attempting to improve the safety of the organization should have immunity from all types of retribution. People, who are unwilling to adopt the culture of the organization and live its values, should be carefully culled. Left unchecked, such detractors will have a devastating effect on the safety and security of the self-managed teams and the organization as a whole.

Each self-managed team should be trained on what a self-managed team is. They should understand the difference between a group and a team. They should understand that they have a shared mission and collective responsibility. They should share insights, information and perspectives. Their decisions should support the collective mission of the team and allow each individual to perform his or her job better. There should be a sense of interdependence and appreciation for complementary and diverse skills within the team. Team members should be encouraged to contribute to decisions and should feel empowered to make appropriate decisions with full awareness of the extent of their authority. They should know when they may need to consult some other member of the team for some decision. They should know how to plan and prepare for absences and team membership changes. Each team member should feel valued and important within the team and know how they are positively impacting the mission of the team and the organization.

Given the large healthcare setting, the CIO should implement an information security office, along with a designated information security officer. This office should be staffed appropriately in order to help implement and monitor security practices of the self-managed teams. One key initiative that this office could help with is the development of a code of ethics which is understood, accepted and practiced throughout the organization by all employees, contractors and partners who are working closely with the organization and handling proprietary information.

Leadership and Ethics within Teams

Each team will need to understand what proprietary information is, their role in its protection, what the possible threats are and how to counteract them. They need to discuss the topic on a regular basis and practice active monitoring of the behavior of all members of the

team to ensure there is no lapse. Protection of proprietary information becomes a shared team goal because any loss affects the whole team. The team's success is determined by the success of all its members. The team could adopt safety practices such as job rotation, separation of duties and implement appropriate access controls which reduce the opportunities for human error and accidental disclosures of proprietary information.

Each team should adopt performance standards and strong processes for bringing on new members, mentoring them, and ensuring that they can be successful within the team. Team members should discuss risks and develop an awareness of the risks of their actions. They should also discuss risk mitigation or avoidance techniques and continuously attempt to improve their incidences of errors. Errors should be discussed along with ways to avoid them and a culture of learning and improving through discussion and reduction of errors should prevail.

Though there may be a designated overall team leader, each team member should be viewed as a leader in some activity and a follower in some other activities. Various roles could be rotated for creating better depth within the organization in order to have smooth transitions as well as to discover better ways of doing something. Such rotations should be accompanied with the removal and granting of access to appropriate proprietary information.

Awareness and Training

Training and awareness programs should be designed around the organizational values so that each member of the self-managed teams can adopt and practice the values within the context of their work environment. One key goal of the training and awareness programs should be to develop a culture of critical thinking – constantly seeking to improve the environment, remaining vigilant, being innovative and always asking the questions: Are we secure? Is this safe? Is

someone trying to trick us? How can we improve the security further? How are changes in our environment and technology affecting our previous sense of security?

Members of the self-managed teams should be made aware of the various threats that they might face. They should develop a culture of trust and responsibility which immediately responds to any threat or possible breach by bringing the matter to the attention of appropriate team members or other leaders within the organization for proper assessment and threat mitigation. They should be made aware of damage control techniques; they should continuously monitor each other's behavior and work diligently to ensure that work is being performed safely and the data are being handled appropriately. This should be done in a mutually supportive way, with the goal of achieving success for the entire self-managed team.

Implications

It should be apparent by this discussion of human behavioral controls that these controls are powerful yet relatively inexpensive to implement. The concepts are simple. However, they require a high degree of leadership engagement and a highly active and ethical role for the leadership at all levels of the organization. Compared to the cost-benefit of technical controls, however, human behavioral controls have a very high rate of return for investment. They are also self-sustaining in the long run – though they may take a high degree of human effort initially. The role of human behavioral controls in achieving an environment which promotes information security throughout an organization can be remarkable.

References

HIMSS Analytics (2010). *2010 HIMSS analytics report: Security of patient data commissioned by Kroll Fraud Solutions*. Retrieved from http://www.krollfraudsolutions.com/about-kroll/himss-security-patient-data-report.aspx

Lussier, R.N. & Achua, C.F. (2010). *Leadership: theory, application, & skill development*. South-Western Cengage Learning, Mason: Ohio.

Probst, C.W., Hunker, J., Gollman, D., Bishop, M (2010). *Insider threats in cyber security.* Springer Science, New York: New York.