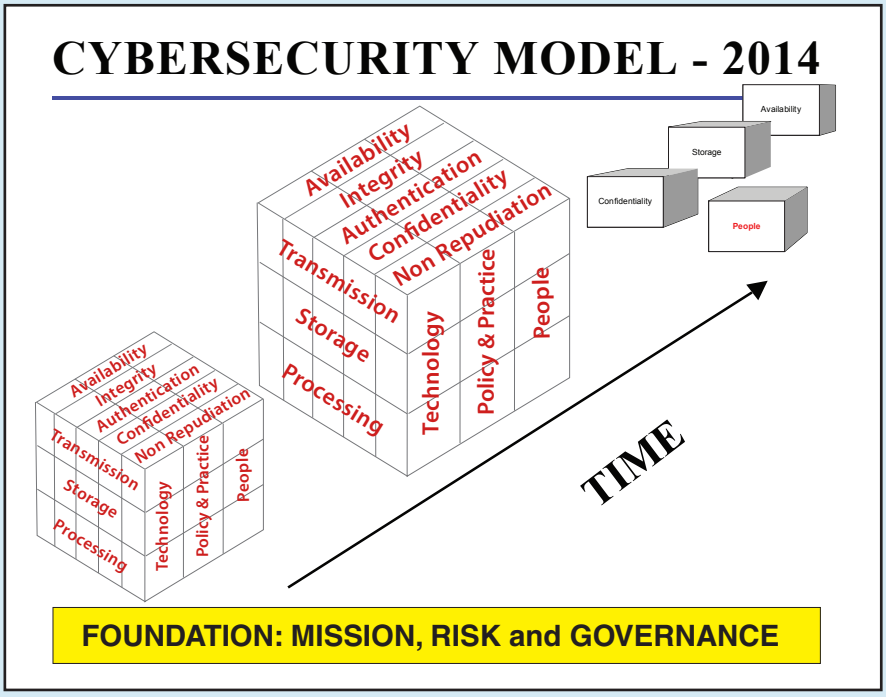
Cybersecurity, Culture and Compliance

by: Dr. Mansur Hasib, CISSP, PMP, CPHIMS
Public Speaker and Cybersecurity Faculty
UMBC

CYBERSECURITY DEFINED

While attending several cybersecurity conferences recently I noticed a lack of a common understanding of what cybersecurity is. I also noticed some confusion between cybersecurity and information assurance. I observed that many cybersecurity professionals and even NIST documents were advocating cybersecurity policy based on the 1991 McCumber model of information security (McCumber, 1991) which advocates "information awareness" programs. My experience has shown that such awareness programs are the bane of the user community and do not really work.

The McCumber model was enhanced in 2001 by the Maconachy, Shou, Ragsdale, and Welch (2001) model which argued the need to manage people for the purposes of information security – which is best accomplished through the cultivation of a cybersecurity culture (Brady, 2010; Corriss, 2010; Hasib, 2013, 2014). While cybersecurity was initially coined as a marketing term, starting around 2010 both cybersecurity and information assurance has been converging into a common concept through the adoption of mission, risk and governance as the foundations of the modern model as shown in the following diagram:



Note. Adapted from "A Model for Information Assurance: An Integrated Approach," by W. V. Maconachy, C. D. Schou, D. Ragsdale, and D. Welch, 2001, June. Paper presented at the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, New York: New York and "Cybersecurity Leadership: Powering the Modern Organization," by M. Hasib, 2014

Mission is paramount because no organization should ever be doing something which does not enhance the mission of the organization and should always be avoiding doing anything that harms the mission. Since we have limited resources, risk management, which includes balancing both positive and negative risks, must be used to determine the priority of our spending on cybersecurity strategy and projects.

In addition, the model must include perpetual innovation and improvement which is also best achieved through culture. Thus in 2014, I offered the following definition of cybersecurity, which was well received by both cybersecurity and non-cybersecurity scholars at various conferences:

"Cybersecurity is the strategic (mission focused) management of information technology and systems which maximizes confidentiality, integrity, and availability of systems and information using a balanced mix of technology, policy, and people while perennially improving over time (Hasib, 2014)."

COMPLIANCE vs CULTURE

One of the problems with compliance is its static nature. The misplaced focus on compliance has been exacerbated by many mandatory laws, regulations and standards. This has been very expensive for organizations and has caused many organizations to digress from cybersecurity governance and the fostering of a cybersecurity culture. Organizations have been forced to spend their limited resources on "being compliant" instead of training people of the use of technology which would improve productivity and innovation. It has also led organizations to view cybersecurity as something separate which has to be layered on top of every effort or project. Instead organizations need to bake cybersecurity into the very fabric, strategy, and culture of the organization.

Compliance also gives people the false sense of security: because an organization is "compliant" with some standard and some third party has "certified" that the organization is compliant, the organizational executives feel secure. Yet, experience has shown that within days or weeks of being deemed "compliant", organizations such as Target have experienced a major cybersecurity incident causing millions of dollars in losses as well as significant damage to reputation.

Compliance does not govern behavior of people – culture does. Focus on culture has high returns on investment for the following reasons (Hasib, 2014):

- Investments in people are cheaper than investments in technology (Weber, Alcaro, & Ciotti, 2001)
- Workforce development enhances productivity and innovation in the organization
- Culture governs the behavior of people (Corriss, 2010)
- Culture is developed and strengthened over time (Corriss, 2010)
- A strong information assurance culture addresses a major source of breaches in organizations (Probst, Hunker, Gollman, & Bishop, 2010)

The stark differences between compliance and culture are summarized in the following diagram:

COMPLIANCE	CULTURE
Expensive	Cheap
Process	Vision
Control	Liberate
Suppress Innovation	Foster Innovation
Lack of Empowerment	Empowerment
Retribution	Reward
NIST Standards	Culture
Governance	Culture
Hire for Skills	Hire for Values
Cost Center	Value Proposition

RECOMMENDATION

In order to achieve lasting cybersecurity with continuous innovation and improvement, organizations must move away from the current focus on compliance and process and focus on people and culture. I hope that future legal and regulatory guidance will foster and support such an effort instead of inhibiting it.

References

Brady, J. W. (2010). *An investigation of factors that affect HIPAA security compliance in academic medical centers.* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses. (Order No. 3411810).

Corriss, L. (2010). *Information security governance: Integrating security into the organizational culture.* Proceedings of the Governance of Technology, Information and Policy, 26th Annual Computer Security Applications Conference, 7 December, 2010, 35-41. United States Military Academy, West Point, New York: NY.

Hasib, M. (2014). *Cybersecurity Leadership: Powering the Modern Organization.* Gambrills, MD: Tomorrow's Strategy Today, LLC.

Hasib, M. (2013). *Impact of security culture on security compliance in healthcare in the United States of America.* Laurel, MD: Capitol College.

Maconachy, W. V., Schou, C. D., Ragsdale, D., & Welch, D. (2001). *A model for information assurance: An integrated approach.* Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, 5-6 June, 2001, 306-310. United States Military Academy, West Point, New York: NY.

McCumber, J. (1991, October). *Information systems security: A comprehensive model.* Paper presented at the 14th National Computer Security Conference, National Institute of Standards and Technology, Baltimore, MD.

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

Weber, B., Alcaro, B., & Ciotti, V. (2001). Avoiding HIPAA hype: Preparing for HIPAA affordably. *Healthcare Financial Management, 55*(8), 62-65.

Dr. Mansur Hasib is the only cybersecurity professional in the world with 12 years experience as Chief Information Officer, a Doctor of Science in Cybersecurity (IA), and the prestigious CISSP, PMP, and CPHIMS certifications. His book Cybersecurity Leadership (2014) shared his leadership model and organizational strategy which he implemented in healthcare, biotechnology, education and energy. His book Impact of Security Culture on Security Compliance in Healthcare (2013) examined cybersecurity in US healthcare. For more information visit: www.cybersecurityleadership.com