Cybersecurity as People Powered Perpetual Innovation

2

Mansur Hasib

Abstract

While tools and technology are important, people are the most important element of a cybersecurity strategy. A properly implemented cybersecurity strategy engages every member of an organization in achieving mission success and in perpetually improving its cybersecurity posture.

Keywords

Cybersecurity governance · Cybersecurity leadership

2.1 Introduction

Cybersecurity is not a one-brain sport. The offensive and defensive cybersecurity capability and ultimate posture of any organization depends on the actions of every individual associated with the organization. While tools and technology are important, the most powerful offensive and defensive weapon for any organization is the collective brainpower of its people [1].

Each human brain is unique. Given the right conditions, each brain has an unlimited capacity to innovate. Brains can also atrophy. Leadership and teamwork can inspire, unleash, nurture, and sustain this force toward a mission. Human brains produce higher levels of innovation when people are happy because happiness produces benign chemicals, which inspire innovation. Conversely, stress and unhappy conditions create an amygdala hijack condition, which significantly reduces a human brain's capacity to think rationally and to innovate. Team and social environments accelerate innovation because social interactions produce inspiration chemicals [2].

Therefore the key to perennial success and superiority for any organization is to implement a culture of perpetual innovation. This requires leadership [1].

People in any organization succeed in fulfilling the mission of the organization most effectively when they can tie their respective roles to the mission. Such connection helps people understand the importance of each role and how the role ties back to the mission. Such a connection inspires better action.

This is the role of risk management and governance, which provide structure, yet allow methodical innovation and the channeling of limited resources towards optimal solutions, which focus on the mission.

2.2 Leadership

Leadership is highly misunderstood. Many academic programs and books incorrectly discuss it and classify it into mystical characteristics and a variety of styles. These sources profess that leaders must possess charisma and several key characteristics, which allow them to influence others. Leadership is often equated to authority and even celebrity status. Some use it synonymously with management. Such confusion results in people believing they are not leaders; nor can they be leaders!

Yet, leaders are not anointed people on a pedestal. Leadership is a frame of mind and not a position. Leadership is also the feeling of empowerment, discretion, and freedom to make a decision and to act. Every person is capable of being a leader. Every person has knowledge, which others do not have. Everyone can use their knowledge to guide others and to gain knowledge from others to make more informed and higher quality decisions and to reduce the risk of their actions.

M. Hasib (✉)
Cybersecurity Technology, The Graduate School, University of Maryland University College (UMUC), Marlboro, MD, USA
e-mail: mansur.hasib@umuc.edu

S. Latifi (ed.), *Information Technology – New Generations*, Advances in Intelligent Systems and Computing 738,
https://doi.org/10.1007/978-3-319-77028-4_2

Leadership through knowledge sharing allows a higher degree of accuracy with a better probability of success; informed decisions are stronger than uninformed decisions. Empowerment allows more decisions and actions to happen at any given time. This results in higher levels of productivity and better outcomes [2].

Every one of us can use our knowledge to guide others and to help others succeed. This is what true leadership is. It can be practiced by anyone and can be the culture of any organization. An organization full of such leaders is a powerful organization!

2.3 People as Expenses

Despite lip service vocalizing people as assets, accounting systems and business schools regard people as simple labor and expenses. Elite MBA schools profess that in order to be successful, executives must discard their emotions; and in their psychopathic pursuit of money and profits—usually designed to benefit themselves at the cost of the organizations, they also toss out their ethical barometers.

In all organizations, including government, people are viewed as the single largest expense and are therefore the bane of Chief Financial Officers. The fact that people produce innovation and are repositories of intellectual capital is largely lost in the vagaries of the accounting system. Therefore, a layoff results in an immediate reduction in expenses; it is frequently used as the first resort. The social and economic costs of the layoff are borne by society and not by the organization conducting the layoff. The intellectual capital loss is not accounted for either.

The professional financial executives groomed by MBA schools are frequently viewed as saviors of organizations and are touted as turnaround executives. The rise to power of these types of executives since the 1970s, has taken an excessive toll on the workforce and the society at large. Gone are retirement benefits, job security, living wages, healthcare, and other key foundational elements required for people to innovate. A culture of annual layoffs, perpetual job insecurity, and unpredictable economic cycles have caused people to worry about their basic needs; people do not have the mental equilibrium needed to inspire innovation and to seek higher levels of purpose.

Chief Financial Officers and Chief Executive Officers with Marketing and Finance backgrounds lead many organizations. Often the mission of the organization or the development of innovative products, which fulfill societal needs and create lasting value for the organization are cast aside in the relentless pursuit of money or profits through cost reduction—usually by laying off people or reducing benefits. Yet, laying off people does not require business genius.

Dramatic levels of corporate consolidation through mergers and acquisitions and other financial games have also driven out competitive forces, reduced investments in people, and dramatically reduced innovation—and even the safety and sanctity of human lives. There has been a general decline in the proportion of US national funds spent in research and development. Even federal research money has declined dramatically.

However, the financial turnaround expert is a myth of dramatic proportions! Examples of these executives causing the demise and malaise of erstwhile healthy or promising organizations such as Enron, AIG, Lehman Brothers, JC Penney, Sears and others are plentiful. Even government organizations, which earlier touted job stability in return for service and a substantially reduced level of compensation are no longer inure from a culture of layoffs.

To facilitate layoffs, government executives have also dramatically increased the use of contractors. Some have argued fallaciously that information technology and cybersecurity are not mission critical and therefore, should be outsourced. While this phenomenon has further reduced job stability for workers, along with a concomitant decline in innovation, it has not reduced government expenses. Rather, it has given rise to large procurement and contracting bureaucracies and actually increased total government expenses; in many cases the expenses are three to ten times more than what it would have been if the government had hired employees.

The situation has been exacerbated further because in an environment of job instability, people are stingy about sharing or documenting their knowledge for the benefit of others; many people view such hoarding of knowledge as job security. The divide in knowledge sharing between the contracting organizations and the government workers is even more dramatic. This is a deadly phenomenon in any organization.

Knowledge in our heads is useless; its power is unleashed only when it is shared. This can mean the difference between someone being able to fulfill a mission or being destroyed in the process. Teamwork and knowledge sharing is at the core of cybersecurity and innovation.

2.4 Ethical Leadership and Innovation

Another serious problem plaguing the federal government sector is the rise of federal contracting companies with unilateral contracts with their workers. These companies require workers to sign away any intellectual property workers may produce. In addition, many of these companies require non-compete clauses for prolonged periods of time, which can take away the ability of workers to earn a living. These companies will purposefully develop a W-2 based employee

relationship simply to avoid paying someone overtime even though they may be billing the government or other clients for the overtime worked by the employee. Therefore, when they can get away with it, these employees refuse to work overtime if they can—often resulting in delays in citizens receiving critical service.

One of the foundations of a free market capitalist society is the promise that if you work hard and you produce great results and innovation, you get to enjoy a fair share of the benefits of that innovation. Certainly the company, which invested in you and provided you the environment and tools, deserves to benefit as well. However, if you are hired with a significant level of experience and pre-existing intellectual capital, there is a serious danger that you will lose rights to your own intellectual capital.

Therefore, with unilateral contracts and a decline in ethical leadership, which promises innovators a fair share of the benefits of innovation, there is no incentive to innovate. People therefore remain unengaged; they clock and bill hours perfunctorily and simply look out for themselves and their next opportunity. Loyalty to the organization has no value and therefore people's association with organizations is temporal. People therefore become a major source of internal threats—both for intellectual property loss as well as accidental and malicious cybersecurity threat vectors. It does not have to be this way! We can and should do something about it. The first step is accepting the criticality of people to cybersecurity and innovation.

2.5 Cybersecurity

Cybersecurity is another highly misunderstood topic. People associate it with computers and networks; they look for a technical solution to every cybersecurity problem. However, cybersecurity at its core is perpetual innovation by people at all levels of an organization.

The mission of any modern organization today is driven by information technology, systems, and data. Therefore their uninterrupted functioning, reliability, access management and protection are critical. In addition, the safety and privacy of legislatively protected data processed and maintained in these systems has to be assured.

Cybersecurity is not a state but a process. Modern cybersecurity has moved from a static 1991 model of information security to a modern dynamic model. In such a model, data exist in three possible states: Transmission, Storage and Processing. Cybersecurity seeks to maintain confidentiality (right people have access to information and the wrong people do not), integrity (information is trustworthy and can be relied upon to make accurate decisions), and availability (information is available when you need it) of systems and information.

We use three tools: people, policy, and technology to achieve cybersecurity goals [3]. However, organizations have limited resources. Every organization has a mission and must prioritize spending so it enhances the mission and maximizes positive risks, which are financially rewarding, while minimizing negative risks, which might harm the mission of the organization. Therefore, mission, risk, and governance are the foundation of an organizational cybersecurity strategy.

Innovation or improvement over time is critical. Through proactive monitoring, refinement, and perennial innovation, an organization can maintain a healthy cybersecurity posture perpetually. Since everyone handles data and information systems, everyone must innovate in their job roles. Everyone must learn to lead as well as follow and a culture of leadership and innovation must exist throughout the organization.

Cybersecurity is the mission focused and risk optimized governance of information, which maximizes confidentiality, integrity, and availability using a balanced mix of people, policy, and technology, while perennially improving over time [1].

A properly implemented cybersecurity strategy engages every member of an organization in achieving mission success and in perpetually improving its cybersecurity posture. The strategy enhances productivity and innovation of all workers of the organization. In addition, such a strategy provides key analytical data and metrics to the executive leadership team so they can maintain executive oversight, actively manage risks, and make optimal business decisions.

As organizations move from the old and static compliance model to the dynamic perpetual innovation model, every organization must be able to perform several key cybersecurity governance activities.

People are the most critical element of all these activities. As a matter of national security, the critical role of people and innovation in cybersecurity has to be recognized and accepted. Devastating cycles of intellectual capital loss, a perpetual state of low innovation and reduced teamwork as a result of contracting and churn has to be obviated.

2.6 Cybersecurity Is Interdisciplinary

Another major fallacy persistent in the minds of many people is that cybersecurity is a Science, Technology, Engineering, and Math (STEM) discipline. Cybersecurity is a business discipline. Disciplinary diversity of people is essential for a successful organizational cybersecurity strategy. People from almost any discipline such as sociology, linguistics, psychology, political science, language, arts, business, law, finance, criminal justice, or forensics can succeed is some aspect of cybersecurity and must be welcomed into the field. Indeed they are critical and cybersecurity education must embrace and teach all aspects of the cybersecurity model.

2.7 The Role of Governance

Governance is another misunderstood topic. Governance is frequently confused with compliance and control. However, governance is simply an organizational framework for ensuring the following [1, 4, 5]:

- Establish Culture and Tone for Conduct [6]
- Provide a Process for Decision-Making
- Establish Accountability, Roles, and Responsibilities [7]
- Establish Strategic Direction
- Encourage and Influence All to Achieve Goals
- Align Risks with Mission
- Implement Effective Controls, Metrics, and Enforcement
- Provides Clarity on Policies
- Provide Avenues for Idea Generation and Prioritization
- Foster Continuous Improvement

Governance requires the engagement of all possible stakeholders for an organization.

Governance must provide a structure, which encourages innovation and safe behavior similar to lanes and other controls on highways.

2.8 People Are Our Greatest Strength in Cybersecurity

People have frequently been maligned as the "weakest link" in cybersecurity. Those who adhere to this jaundiced view, resort to more control, cybersecurity awareness programs, and surveillance of people, which create a police state and stifle innovation.

Cybersecurity, by itself is meaningless and irrelevant to most people. Training must be relevant to the jobs people do. Training should stress job relevant technology usage and associated data safety practices. Forcing people to take cybersecurity awareness training, based on an outdated 1991 information security model, is dubious.

Phishing tests have dubious results as well because people fall for such schemes due to an amygdala hijack condition and the only way to fix this is to train people to move away from the stimulus even for 10 s before doing anything so that the chemical reaction caused by the amygdala hijack can subside [1]. People should be rewarded for ideas, successful innovations and improvements. People do not respond to purely negative policies.

2.9 Recommendation

Based on the principles identified in this paper, use cybersecurity leadership to implement a people powered perpetual innovation strategy as a lasting offensive and defensive cybersecurity strategy.

References

1. M. Hasib, *Cybersecurity Leadership: Powering the Modern Organization*, 3rd edn. (Tomorrow's Strategy Today, LLC., 2015)
2. K. Zachery, *The Leadership Catalyst: A New Paradigm for Helping Leadership Flourish in Organizations* (Bravo Zulu Consulting, LLC., 2012)
3. W.V. Maconachy, C.D. Schou, D. Ragsdale, D. Welch, A model for information assurance: an integrated approach, in *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, United States Military Academy, West Point, New York, 5–6 June 2001, pp. 306–310
4. L. Corriss, Information security governance: integrating security into the organizational culture, in *Proceedings of the Governance of Technology, Information and Policy, 26th Annual Computer Security Applications Conference*, United States Military Academy, West Point, New York, 7 December 2010, pp. 35–41
5. T. Schlienger, S. Teufel, Information security culture: from analysis to change. S. Afr. Comput. J. **31**, 46–52 (2003)
6. T.E. Deal, A.A. Kennedy, *Corporate Cultures: The Rites and Rituals of Corporate Life* (Addison-Wesley, Reading, 1982)
7. A. Dutta, K. McCrohan, Management's role in information security in a cyber economy. Calif. Manag. Rev. **45**(1), 67–87 (2002)