

Chapter 16 Executive Communication

Chapter Objectives

This chapter will discuss:

- The importance of visible executive support for security initiatives,
- Ronald Coase's theory of Transaction Cost Economics,
- Harvey Leibenstein's theory of X-Inefficiency,
- Mari Sako's theory of Trust, and
- The application of these theories to an organization's security.

16.1 Executive Communication is Crucial in Shaping Employee Behavior

While the communication an employee internalizes most comes from their direct supervisor, as will be discussed in the following chapter on training, executive communication plays a major role in establishing an organization's priorities. This does not mean, however, that a single email or memo from the owner or CEO will be enough to change frontline employee behavior to conform to the required standards to protect network security. Top-down direction is necessary but not usually sufficient to ensure compliance with any direction. Because workers perform in accordance with how they are evaluated and rewarded, it is important to not only publish statements mandating that certain actions be taken but that the people in charge of implementing the processes have their evaluation and pay criteria based on fulfilling the mission as newly defined. The areas of responsibility can be thought of in the following manner:

First, the business processes of the organization and the responsibility for executing those processes should be assigned from the most senior levels of the organization to the line employees actually doing the work. As discussed in Chapter 10, the processes are comprised of *people* who belong to *organizational units* performing *functions* as part of a *business process*. At the executive level, parties should be put in charge of implementing business processes and should be, whenever possible, in charge of

the functions performed in support of their process. When it is not possible for one person to be in charge of the entire business process, they should be required to coordinate as often as necessary with those responsible for the functions. In addition, overlaps between processes (functions that support more than one business process) should be identified and those responsible for each process should also coordinate to ensure all business processes are able to be implemented satisfactorily.

Second, an Executive Committee comprised of the senior executives in charge of business processes should be formed and should meet regularly (monthly is a good start and can be adjusted as necessary) to discuss security-related issues. As issues are identified either by executives or by others in the organization a process for tracking the issues to resolution should be implemented. The issues should be evaluated according to their difficulty, time estimated to complete, policy decisions or waivers that must be obtained, and “downstream” processes or decisions impacted by the decision. If possible, a preferred solution should be suggested. The first priority, however, is that the issue be stated clearly and concisely but completely. A single person should be in charge of ensuring the issue is resolved and status should be reported regularly. A common policy is to require that overdue or problem issues be briefed to the Executive Committee when required.

Third, sub-committees and working groups should be assigned to implement the business decisions made by the Executive Committee and to determine how the directives should ultimately manifest in practice. In the U.S. public sector, this is analogous to what happens with a law. The law, which is a high-level policy decision, is passed by the legislative branch and signed by the President. After the law is enacted, however, the executive branch agency responsible for overseeing the law’s enforcement must draft regulations which must be followed in order to be in compliance with the law.

Now that the business processes, senior-level committees and working-level committees have been discussed, it is important for the theoretical underpinnings of an organization’s actions to be addressed. Because an organization’s profitability or effectiveness is tied to its ability to perform its business processes efficiently, Transaction Cost Economics is mentioned. Because many transactions are implemented either entirely or in part by humans X-inefficiency is mentioned. Finally, because the safeguards required to ensure security is being properly maintained are based