FEBRUARY 2022

INFORMATION SECURITY IN LARGE ORGANIZATIONS

PROTECT COMPANY NETWORK & INFORMATION

WHEN TO DISCIPLINE EMPLOYEES FOR INFORMATION SECURITY VIOLATIONS?

We hear, and come up with ourselves, about minor violations of security procedures all the time. An employee who gave his password to his friend. An employee who did not pass an employee card on an attendance clock. Employees who found a way to bypass the block to Facebook. Should we take care of such a case anyway? Should there be room for discretion? And if by chance in one month you have already dealt with two such cases, should you deal with a third incident that you have encountered? Or is it already too much and will lose its effectiveness?

How much to adjust the balance of horror to the personality in front of you and how much to be consistent regardless of the character in front of you?

HOW TO HANDLE EVENTS?

Will each event end in a hearing (according to the procedure) with senior executives (with a chance of concluding the deal or a comment in the personal file)? Or talking one-on-one with the recalcitrant employee in some cases? (For employees it is a negative resonance.) Employees are afraid to commit similar offenses. On the other hand, too many such hearings and the information security manager is perceived as bloodthirsty and a bad person.

Will an underestimating employee who is not interested in 'these risks' cause you to land instructions firmly?

While a nice and gentle employee who does not excel in project management and does not bother to remember that having to integrate information security will make you try to calmly explain to him repeatedly the information security requirements?

It is not easy to strike a balance between the balance of terror and the use of authority and the attempt to conduct oneself as business units (even though information security does not generate revenue) in the organization. It is also very difficult to measure where we are on this scale. Do we tend to work by force (extensive use of procedures and controls) or managers as a service-providing unit (hear about information security not only in handling events but also as a contributing body to product development or sales campaign)?

Informal conversations with employees, managers and external auditors, provide an opportunity to understand how effective the actions we take, are. The very fact that junior employees consult with information security as to whether a particular action is permissible, and how to perform it, indicates that they have internalized not only the importance but also the awareness of the various risks.

Managers who approach security managers on their own initiative to report irregularities in the organization have probably internalized the importance of information security for the organization. Project managers who want information security to feature a secure solution early in the project not only save themselves a headache, but also money at the end of the project.