The Internal Threat

Tal Sar-El
September 2021
Metzuda , Issue 41, page 26
View on Linkedin

The internal, intra-organizational threat is one of the most challenging threats in any institution, organization, and society. The damage can be economical, relating to the organization's image, and have a devastating effect on the organization itself or another institution to which it provides a service, sabotaging its functional continuity and sometimes even causing it to collapse.
The management backbone of the organization plays a vital role in determining the policy of dealing with the issue of internal threat.
In this article, I will present my outlook regarding the ability and tools of an organization manager in general, and the security manager in particular, to better deal with the internal threat and the potential damage that results from it.

Several weeks ago, the media exposed an event called the **"Intelligence Officer Event."**

From the media, we can learn about a severe indictment filed in September 2020 against an officer who served in the Intelligence Division technology unit in the IDF. The officer was under detainment until the end of the proceedings. Sadly, during his stay in a military prison, the officer was found dead in his prison cell. The officer, 25 at the time of his death, was a gifted boy. During his high school studies, he studied computer science at university, received a bachelor's degree, and was an employee of a large high-tech company.

According to the IDF Spokesman, the officer consciously committed several acts that severely damaged state security and, during his interrogation, admitted many of the actions attributed to him. The investigation further revealed **that the officer acted independently, for personal motives and not for ideological, nationalist, or economic reasons.**

The chief of staff, Aviv Kochavi, clarified that there is no similarity between the incarceration of the officer and the affair of "Prisoner X" and that he "committed severe offenses. He did them on purpose, for reasons I can not describe. He almost exposed a big secret, and we stopped it in the 90th minute. "
This affair presents us with the potential for serious harm that may occur from a person within the organization who commits acts that have the potential to cause severe damage, not out of betrayal or greed but out of personal motives.

From a broader perspective of personal motives, the issue can be characterized by various characteristics, from curiosity and inquiry to desire for revenge due to inappropriate treatment.

The question here that arises is **what is a manager's role, and what are the tools in the hands of a manager in general and a security manager in particular in dealing with the internal threat within the organization?**

The damage from the internal threat, whether caused by accident or malice, often crosses the criminal threshold, is more extensive than attributed to it, both in the identity of the 'enemy' and in the characteristics of the 'Possible course of action.' It is an enemy that does receive the clear definition as an 'enemy' in the first place. In practice, this could be one of the employees, service providers, suppliers, and various factors in the supply chain or any other aspect that maintains interfaces with the organization.

As part of protecting against the internal threat, many organizations are adopting the concept of **'Zero Trust.'**
This concept, taken from cyber protection, is based on the fact that security in the organization gives zero confidence (Zero Trust) in the employee and raises the protective walls of the closed internal network. The basic assumption is that violations and loopholes exist within the organization's work processes and systems. Therefore every request for entry and transition between internal systems must be re-verified, including the person whose entry into the system was approved, and each entry into the system originates from an external open network.
It means that 'Zero Trust' requires continuous authentication, maximum segmentation and compartmentalization, and minimum access permissions.

Yet, though this method is being in use for years, we see an increase in incidents where organizations experience damage originating from within the organization. Moreover, the source of this type of damage is not limited to the cyber realm.

The Ponemon Research Institute[1] is an American research institute that collaborates with various organizations and deals with research and education to promote responsible usage of information and management methods on privacy in businesses and government institutions.

The findings taken from a report by the Ponemon Research Institute, sponsored

[1] https://www.ponemon.org/

by *OBSERVEIT* and *IBM*, show that during the two years between 2018 and 2020, the number of cases in which organizations experienced damage from internal factors soared 47%[2]

There is an unassailable consensus that the internal threat exists, and its danger can be existential. Still, being human, it is difficult for us to deal with it personally, as it sometimes requires us to cast suspicion and blame on co-workers, some of whom even form part of our social circle in our spare time.

The conduct in the COVID-19 reality, the situation in the economy, and how remote work is becoming more common have put us in front of the demand to "take" the computer system outside the organization's walls. In this situation, we increase even more the potential for damage from internal 'enemies.'

A study conducted by Code42[3] in collaboration with the Phonemon Institute, which addresses the internal threat of 2021, highlights the need to adopt a new approach in information security and the need to invest in modern insider risk technology. Furthermore, the study revealed the leading causes of the growing problem of internal threat, including post-COVID-19 data loss analysis and the challenges in constructing a plan to address these risks.

The main findings of the study indicate that:

- Today, employees are more likely to leak files than they were before COVID-19.
- 54% of organizations do not have an internal risk response plan, and 40% do not understand how ineffective their technologies are in dealing with an internal threat and even facilitating damage within the organization.
- 59% of IT security managers expect internal risks to rise in the next two years.

Required directions of action:
As a first step in dealing with the internal threat, the organization's management levels must recognize that such a potential exists and understand the need to address such a threat.

Managers in general, and security managers in particular, must bring to the surface these questions:

- What are the new challenges that are creating new threats?
- What are the weak links in the organization?
- What are the ways to reduce the potential for danger and harm?
- Have we provided all the relevant parties with all the appropriate tools for dealing with the threats?

They must ask focused questions in an attempt to bring to the front the weak links:

- Who is the employee without whom it is impossible to get along?
- Who is the employee who controls the details and luckily knows all the little details?
- Who is the employee that some customers prefer to work only with that person?

---

[2] https://www.observeit.com/2020 Global Cost of Insider Threats Ponemon Report

[3] https://www.code42.com/2021 data exposure

- Who is the non-organizational factor that has a "deep" connection to the organization?

Examination and analysis of the organization is the basis for finding solutions to reduce damage from internal threats and solution implementation, including the organization's nature, workforce, the hierarchy of roles, processes, and procedures. It is an inside-out, including the factors that interact with the organization at all levels. Such inquiry will flood the weak links and gaps, vulnerabilities, and loopholes. Early marking of these vulnerabilities will allow management to focus on:

- Building work processes
- Outline an orderly coping plan
- Allocation of resources for policy implementation and ongoing control

The answers to these questions are the key to dealing strategically and tactically with the internal threat.

In light of the research findings, it is clear that the 'Zero Trust' method, which presents a rigorous conception of security in the organization, especially in the face of internal threats, does not provide a satisfactory solution. The organization's management should see it as one component in the chain of measures for protecting and dealing with the internal threat and not as the only or central component in protecting the organization.

The security manager, who is in charge of this domain, should build a plan based on a periodic review, examination, and analysis of the weak links of the potential threat to enable ongoing confrontation with them. In addition, it is essential to initiate occasional moves that serve as "Routine Disruption" actions, such as: making changes in the organizational structure, changes in the posts and positions, in the placement of employees in front of customers, in the process of approving suppliers, as well as in procedures and guidelines.

At the same time, the security manager must take care of an organizational routine in the field of 'internal threat,' a routine that includes:

Training: Establishing and implementing an annual training program for employees to increase their awareness of the issue of internal threat and to provide tools and procedures to reduce it. It is important to emphasize that performing a single instruction or practice to fulfill one's obligation is ineffective, both in obtaining a more reliable picture of the area and in the deterrent effect on the employee, who feels that this is an action aimed at marking the execution line. The security manager needs to implement a plan to maintain and strengthen vigilance to become part of the routine over time.
Control and audit: Construction and implementation of an annual audit plan in different frameworks and levels of testing, which will examine the organization in a wide and varied range of scenarios. An audit will make it possible to identify weak links in real-time, and at the same time, preserve and strengthen vigilance.

Investigation: The security manager, backed by the organization's management, must instill an organizational culture of conducting inquiries, the purpose of which is learning and improvement and not a "search for culprits." Conducting investigations in real-time can improve processes and reduce vulnerabilities in the organization and should be carried out at all times, in cases of "almost

happened" and not only after the damage has occurred.

Technology: The use of various protection technologies can perform real-time monitoring in cases of violations and anomalies in workers' conduct and other factors in the supply chain. Incorporating appropriate technology can reduce in high percentages the potential for damage that internal factors may cause.

In conclusion, dealing with the internal threat can be challenging, even Sisyphean, since the opponent is in the house. In many cases, it is transparent and even seems non-threatening. About 61% of the damages caused by internal organizational factors occur inadvertently, starting with errors, out of distraction, due to neglect, through negligence, and disregard for procedures.
The potential for damage from internal factors is immense, and in extreme cases, it can undermine the functional continuity of the organization and even cause it to collapse. However, through annual, structured, and systematic plans, it is possible to reduce the potential threat and harm.
It is necessary to note, however, that without the recognition of the organization's management, that there is an internal threat, and without providing backing to those in charge of implementing work plans in this area in the organization, including security managers, the ability to apply procedures, guidelines and policies is limited. Therefore, recognizing the threat, the potential for harm, and the cooperation necessary in dealing with it is the basis for effective and quality facing the issue.