

Managing Security Related Risk

If it seems that large and small organizations alike are reporting a significant rise in inventory losses due to unauthorized, after-hours access, it is not your imagination, the pharmaceutical industry reports that these types of heists in the U.S. have quadrupled since 2006. Despite the best efforts by company officials after the fact, these loss events have quickly catapulted the victimized organization into an unfavorable spotlight that most often has resulted in an immediate loss of reputation as well as a general lack of confidence in the organizations' stock price. Typically, these events are initially reported in the media as being the daring, random acts of reckless individuals that seem to have beaten all the odds against the victim's protection strategies. However, when a closer look is taken one will find that these events were anything but reckless or random. These acts are in fact specifically targeted events against the victim by an informed team that knew in advance exactly what they were going to do.

Recent research suggests that the root cause for many of these loss events can be directly attributed to control / process breakdowns in one or more of the following areas:

- Insufficient Staffing / Training
- Negligent Hiring / Retention / Supervision
- Security Equipment / Technology Failures
- Security Program Reduction
- Violation of One's Own Standards
- Violation of Industry Standards
- Failure to assess the overall risk and implement appropriate security measures

Although all of the above causations can be significant contributors to a control / process breakdown, the failure to assess the overall risk of the organization is, in my opinion, the most critical. When an organization fails to identify its own vulnerability it guarantees that the organization will be exposed to an unknown frequency and severity of peril.

Currently, the security industry leading practice points towards the use of the ASIS International General Security Risk Assessment Guidelines, first published in 2003, this process provides an overview and background of Risk Assessment Methodology that leaves room for interpretation and customization for all business types.

Risk Assessments should be continually performed in order to identify the sources of risk, know your organization's weaknesses, and anticipate a response. Once identified the organization should obtain the tools and advice necessary to avoid the risk.

If the organization cannot avoid the risk the best effort should be made to lower the impact of the event. After the event steps should be taken to resolve and recover from the event. Lastly, it is important to learn from the event, identify the process or control breakdown, make recommendations and share the results to avoid future occurrences.

In closing you should know that not all potential events can be avoided or significantly mitigated. Keep in mind that incidents may still occur despite your best efforts. It is also true that sometimes nothing happens in a risky environment. When incidents occur at a high-risk location it does not necessarily indicate negligence on the part of the organization. Lastly, a lack of incidents/events at any one specific organization or location is not necessarily evidence of a good security program.