PRIMORIS
ASSOCIATES INC.

Threat, Risk and Vulnerability Assessments – Why?

White Paper

THE FOUNDATION OF ALL SECURITY

> All security measures flow from the threat and risk assessment (TRA). If one does not know with a high degree of certainty what is to be protected in the organization and its value, it will be difficult to choose the correct protective measures to prevent these assets from being lost. If one cannot establish a list of vulnerabilities and their severity, applied protective measures may be inappropriate or ineffective. If one does not understand the effectiveness of existing security measures, all assets are placed at risk. And finally, if a methodical approach is not taken to understand the threats to the

> assets and the organization, otherwise effective security measures will fail. The threat and risk assessment will determine all of these things.
>
> In our business, we have seen a great variety of approaches. Often, an organization will occupy a building and will be handed keys, an access control system, an alarm system, and a camera system provided by the architect. This approach has a number of obvious flaws: the architect does not know enough about your core business to design protective systems and generally will design only a system for the base-building; often, the organization does not have a security professional in its hire and Facilities will be responsible for security; no methodical approach has been applied to business operations to right-size security. The real solution to this is the TRA.

The threat and risk assessment is the pediment for all security measures.

Security by Non-Security-Trained Personnel

What we have frequently seen is that a subsequent breach of security will lead a non-security-trained manager to perform “security by walking around.” In this case, there has been a break-in or a theft and a manager now examines the area and indicates where new cameras and new intrusion sensors will be placed by pointing a finger. Occasionally this will be accompanied by a guard force for a period of time or some other new security modality. For us, this is like having a non-doctor directing a surgery. The result will be expensive and not terribly effective. After such an exercise, someone might eventually suggest that a security professional could have some insights and we are often invited to do a “security review.” In this exercise, the company expects that we will look at all the security measures in place and make a pronouncement on whether or not they are adequate. While this is an opportune time to explain and recommend a TRA, involving security professionals at the design stage is the most effective and economical.

TRAs use Known Methodologies

Professionals have access to a variety of Threat and Risk Assessment methodologies. Since we have done much work with the federal government, we are familiar (very familiar) with the Harmonized Threat and Risk Assessment Methodology (2009). We are members of ASIS International and are familiar with its methodology. We have CARVER1 (Criticality, Accessibility, Recoverability, Vulnerability, Effect and Recognizability). Australia and New Zealand to have a very credible AS-NZS 4360 Risk Management tool. MSHARP (mission, symbolism, history, accessibility, recognizability, population, proximity) is also a popular tool which is similar to CARVER and is especially useful in military circles. We have used methodologies provided by banks and nuclear facilities. We maintain a list of 15 methodologies for Information Technology systems.

Whichever one you choose, the process and the result should be similar. Each one will require a methodical approach to: identify and evaluate assets, assess security systems, analyse vulnerabilities, and discover all existing threats. Once this information is known, risk can be calculated using a common risk formula R f Aval, T, V (Risk is a function of Asset value, Threats, and Vulnerabilities).

Let's look at each component in turn.

The Essential Components of the TRA

Assets are the central reason for security. If an organization has nothing of value, nothing needs to be protected. A store that sells second-hand clothing from donations does not need an advanced intrusion detection system and security cameras, indeed this cost could not logically be justified in the bottom line. Then, understanding the value of assets is the foundation piece of the TRA.

TRA Categorizes Assets

Most TRAs put assets into four categories: physical things, people, information, and tangible things. The physical resources that a business needs to operate can all be assigned a dollar value but all things are not counted in a TRA. Including physical assets of minor value like desks and chairs and computers will only cloud the results. We include buildings, IT systems, vehicles, large equipment, etc. Generally, a dollar-value cut off is assigned depending on the relative value of all assets. We have used figures as low as $4000 and as high as $100,000. Physical assets can also have an intrinsic value; by this we mean a value that is greater than the dollar value. For example, we once did a TRA where a lab technician pointed to a $300,000 electron microscope indicating that it was the costliest piece of equipment in the lab. But he quickly followed up by pointing to another piece of equipment with a relatively minor value saying that if he did not have this piece of equipment, he would not be able to do his work. This is intrinsic value. Critical spares and the just-in-time supply system fall into this same category.

People – the Challenging Asset

People present a difficult question in TRAs. All companies tend to use the mantra “our employees are our greatest assets.” While this is undoubtedly true, for the TRA, humans do not have a high value. We tend to say that if an employee performs a critical role such that if he or she were plucked from the organization the organization would stop or at least shudder, then that employee has a high value. We do not find many of these in any organizations. In fact, such a situation would create a vulnerability for the organization. We also consider groups of employees to have a higher value, e.g.: all of the senior executive; all of the engineers. We often recommend a travel policy that prohibits all of these people from travelling together on the same mode of conveyance because of the vulnerability created. In any case, humans do not have a high value in a TRA and this subject must be broached carefully with the client. One can just imagine the problem for the TRA if a company had 500 high-value, ambulatory assets

Information as an Asset

Information generally has a high value in an organization but because few private companies subscribe to information security classification systems, this is often difficult to establish concretely. We give higher value to information which has a higher sensitivity. Governments are well-versed in this. They use a schema to classify information so they can understand how it needs to be handled, i.e.: created, transmitted, stored, disposed-of. Private companies generally do not make the effort to create such a classification system. Nonetheless, the role of the TRA analyst is to identify this as an issue and recommend information security classification systems, even rudimentary ones.

What About Intangible Assets?

Intangible assets must be identified and evaluated. Intangible assets are such things as the company’s reputation; its credibility within the community; people’s feeling of well-being while at work; and the value of its brand. As one can imagine, these are difficult things to evaluate. Our experience is that we find professionals working in companies and applying skills to the best of their abilities. For them, their reputation, and therefore the company’s reputation, has high importance. We find organizations conducting processes of which the local community may be wary and they realize the significance of the social license which has been granted to them to operate. We also understand the value of contented employees and the importance of their feeling of well-being while at work. We tend to rate all of these things as high and sometimes a very high depending on the sensitivity of the operations of the business, e.g.: mining, nuclear processing, etc.

Security by Walking Around Won't Work

The remaining components of the threat and risk assessment will be the subject of future papers; however, we thought it appropriate to discuss these initial facets of threat and risk assessments. Because of the number of TRA's we have performed, we are fervent believers that "security by walking around" by non-security-trained managers can never be effective. We also believe that creating true security requires a professional approach by professionals. We have seen many organizations which have required the facility's people to brush up on security and try to sustain it. We have also seen security assigned to health and safety professionals but this is always something done half-heartedly off the corner of their desks. We have seen organizations turn to their contracted security guard force for advice on corporate security. We cannot imagine how this could ever function.

In Conclusion

The threat and risk assessment is the pediment for all security measures. It is a methodological approach to identifying all assets to be protected and all elements which can create risk. It should be performed by a trained, experienced security professional and all recommendations should be assessed for a return on investment and a schedule for when they will be acted on. After applying all recommendations, there will be a residual risk and this risk should be the subject of a register that is reviewed monthly by management. We hope that this short article brings some clarity to this important topic and makes you reflect on your own risk posture in your business.

Office: 514-418-4609 | info@primorisinc.ca | www.primorisinc.ca