HARVARD
Information Security

Information Security Risk Assessment

Introduction

A risk assessment is an important part of any information security process. A risk assessment is used to understand the scale of a threat to the security of information and the probability for the threat to be realized. The result of a risk assessment can be used to prioritize efforts to counteract the threats. The following scenarios illustrate how a risk assessment will assist in making information security decisions.

Scenarios

A printed list of all Harvard employees with their names, addresses and social security numbers is left in a public place for a courier to pick up on a weekly basis.
A printed list of HUIDs, with no names or any other information, is intended for an external consultant and dropped into a mailbox.

Risks

Risks are present in both scenarios; the first scenario presents a far greater risk than the second. In the first scenario, detailed information suitable for identity theft on many people would be exposed if someone were to steal the printout. It would be easy to do so since it is left in a public place for pickup. In the second scenario, only a few confidential HUIDs, not easily used for identity theft, might be exposed. The US mail system is quite secure so it would be difficult for someone to steal the letter. In the first scenario the scale of the threat is high and the threat probability is also high. In the second scenario the risk and threat probabilities are both low.

Recommendations

Efforts should be focused on mitigating risks such as that in the first scenario. These efforts may include reducing the information that is transported, (for example by only sending information about new hires using HUIDs to identify individuals) or by securing the transport, through use of an encrypted file transfer for example.

In some cases the risk may outweigh the value of the function and the best solution is to stop the function.

Only after significant threats are mitigated should users focus on any low risk situations. In some cases the risk of exposure or exploitation will be low enough that the cost of mitigation outweighs the risk.

Conclusion

Performing a risk assessment will help determine where to focus resources, when to think about modifying functions, and when to stop using that function as the risks may not warrant corrective action.