ASK THE QUESTION

WHAT IS MY SECURITY STRATEGY?

Introduction

Security is often thought of as a tactical issue that should remain at the "gates and guards" level. While these tactical security pieces may be important they are most effective as part of a security strategy that is designed to mitigate the threats and risks to your company and its operations. True security strategy is integrated into a company's "C Suite" and is seen as an enabler. The questions and discussion that follow outline the framework for a company security strategy.

What is the Threat?

Designing a security strategy starts with getting a true picture of the threat to your company and its operations. This should start with a general look at overall threats in your country and industry and then moving to the more specific such as trends in security incidents that have happened in your company or in close proximity. Threats are examined from the perspective of likelihood of occurrence and impact to your company should they occur.

Once the threats and risks are known then they need to be examined against the security measures currently in place in your company. Are your current security measures adequate to protect against the most likely threats that would have the greatest impact on your company's operations. If not, then what needs to be done to close the gap?

Common Findings

Presidia has conducted many threat risk assessments or security reviews for a wide variety of clients. Typically, the findings fall into the following areas:

Governance

Often security is decentralized without a senior position designated to provide oversight. This can result in inefficiencies and inconsistent application of security measures across company operations. Inconsistency can mean not enough security but it can also mean that there is too much security in an area where the threat does not warrant such measures.

Policy

Security policy is often non-existent or limited in that it is spread out amongst many other policies and as such is hard to find.

Training

Many companies do not have a formal security training plan to cover topics such as emergency response, information protection and security awareness.

Response

Companies frequently respond to a security incident as a “one of” meaning that the incident is not formally tracked, statistics are not kept and there is an absence of a lessons learned program.

Recommendations

If the above findings describe the current state of your company’s security program fortunately it does not have to be difficult to fix. A formal process conducted by a security professional either from within your company or contracted specifically to conduct a security review can give you an accurate picture of the current state of security in your company and what additional measures, if any, should be implemented. If you don’t have a senior security professional on staff and contracting one in is not practical, then consider a self examination using the guidelines below.

Governance

- A senior person should be designated to provide oversight of the company’s security program at the strategic level.
- A formal reporting mechanism should be established for reporting security incidents.
- Thresholds should be established to determine what incidents may pose a serious risk to company operations. These incidents should be reported to the senior security person ideally at the VP level.

Policy

- Security policy should be in one place and written so that it can be understood by an individual who is not a security professional.
- Security policy should describe the security governance guidelines for the company.
- Security policy should recognize related programs such as business continuity.

Training

- There should be a formal security training plan.
- This plan should identify who needs to be trained and how often.
- The plan should identify a communication mechanism to ensure that emerging risks and appropriate mitigating measures are identified and communicated to those who need to know.

Response

- Security incidents should be recorded and tracked.
- Statistics on security incidents should be kept to identify potential trends.
- A lessons learned program should be adopted to review serious incidents and recommend changes to policy or procedures if appropriate.

Conclusion

Asking what your security strategy is or what is should be does not have to be an expensive or complex endeavour. Putting some thought into this question will enable you to make security decisions from a position of knowledge to ensure that security measures in your company are cost effective, lower your risk and enable your company's operations.

About the Author

Stephen MOORE

Stephen Moore is a police, security and emergency management professional with over thirty years of experience. He has worked with all levels of Government and with police and security agencies both domestically and internationally. Highlights of his career include leadership of the security program for the Department of National Defence and service as the Canadian Forces Provost Marshal (Chief of the Military Police) leading an organization of 2000 members delivering policing, security and criminal intelligence services both in Canada and abroad. Stephen is currently the President of Presidia Security Consulting.