Governance & Risk Management

PREPARED BY MARTIN LEE AND JON MUNSHAW

Updated October 21, 2019

TALOS

CONTENTS

INTRODUCTION

Businesses are built on risk. No matter how prepared they are, there is no guarantee that any decision will result in the expected outcome. But through good management, the likelihood of success can be improved.

Risk management is the art and science of understanding risk. Good risk management recognizes that risks can never be completely removed. However, resources can be allocated to both reduce the likelihood of an adverse event occurring, and to minimize the consequences if an adverse event does occur.

Governance is the process by which decisions that affect the business are made, recorded and implemented. Risk management feeds into the governance process allowing management to understand their exposure to risks, and judge if these risks are being appropriately mitigated.

Cyber security is an evolving domain; the nature of cyber risks is constantly changing. CISOs need to ensure that the process by which they come to decisions regarding the mitigation of risks is adequate to the challenges they face specific to their own environments.

THE PROBLEM

Adversaries are aware of the opportunities that networked computer systems — and the data that they hold — present. Criminals seek to make illicit financial gain, state-sponsored adversaries seek to advance their geopolitical interests. Both types of adversaries can satisfy their goals through the compromise or destruction of these systems.

In a world of finite resources, it's not possible to protect everything. Nor is it desirable to over-protect systems to the point of preventing growth. Levels of protection and defenses must reflect both the risks faced by systems and the consequences that may occur if an attack against a system is successful.

These risks are in constant change. The protections deployed in the past may no longer be adequate due to changes in the threat environment. Hence, risks and protections must be regularly reviewed.

The threat environment can change suddenly. For example, in June 2017, the NotPetya destructive worm was released via the compromised software update system of a legitimate software package. The attack was almost certainly associated with the geopolitical situation in Ukraine. However, the malware spread across the globe, destroying computer systems, and becoming the most costly attack in history.

This attack happened shortly after the WannaCry worm showed how damaging self-propagating destructive malware could be, and after many years of ransomware attacks rendering systems inoperable. At the same time, organizations had become increasingly reliant on computer systems in order to operate. Yet many organizations failed to analyze these changing risks and deploy suitable protection to protect against such an attack.

THE SOLUTION(S)

Governance is a vital function of any security management program. CISOs must be aware of the systems they are protecting, their importance to the organisation, the risks that they face, and the consequences of a successful attack on the organisation. CISOs should be able to describe the risks and consequences to their leadership in a way that they can meaningfully understand so that these risks can be correctly mitigated and managed.

An effective culture of security and responsibility helps integrate the principles of security and risk to all levels of the organization. Providing clear enterprise standards and policies that define processes and procedures with assigned roles and responsibilities allows staff members to understand what it is that they are expected to do, and their role in securing the enterprise.

In a world of finite resources, it is not possible to completely protect against every threat to every system. Systems and threats need to be prioritized. Wider management should make informed decisions regarding levels of security and be comfortable with the choices and potential consequences of these choices.

Security should be an enabler of progress rather than a stick-in-the-mud that frustrates the development of new systems. Creating a culture of security and spreading awareness of current threats

All of this should be driven from a formal process of risk management by which systems can be properly assessed for risk, the consequences of a successful attack quantified, and suitable mitigations put in place. Necessarily, risk management is a dynamic process as new risks become apparent previous decisions regarding suitable mitigation need to be revisited.

CONCLUSION

Quality security depends on a good understanding of the risks and what is at stake. This, in turn, depends on the presence of an appropriate risk management program.

There are many different published risk management and governance frameworks. Implementing an appropriate standard within your organization will go a long way to setting up a solid security foundation.

The news is littered with reports of organizations that failed to deploy adequate mitigations against known threats and who have suffered the consequences. Reviewing these events and using them to evaluate how your organization would respond to such a threat is an excellent starting point to examine existing tolerances to risk and current levels of protection.

ADDITIONAL READING

Governance

- NCSC, 10 Steps to Cyber Security - A board level responsibility
- ISACA, Information Security Governance: Guidance for Boards of Directors and Executive Management

Risk Management

- SABSA, Risk Management Part One - The Meaning of Risk
- NIST, Risk Management Framework Overview
- ISO, ISO/IEC 27005:2018 Information security risk management

CHECKLIST

We have built a simple checklist to help you quickly access these issues in your organization:

ID	Item	Y	Description
Governance			
	Is the board regularly briefed on cyber risk?		Gaining board-level visibility and engagement with cyber security is vital to ensure the issue is given the attention it warrants.
	Are the board and management satisfied with the level of risk to which they are exposed?		Boards need to be aware of the level of risk to which they are exposed, and comfortable with the level.
	Are decisions on risk and mitigation agreed and recorded?		Recording decisions allows these decisions to be reviewed at later dates and makes clear what mitigations are required and why.
	Does everyone in the organization understand and value their role in cyber security?		Security is everyone's role. Promoting a culture of security throughout the organisation helps permeate security into everything that the organization does.
Risk Management			
	Has a Risk Management process been adopted for projects?		From the outset, any project should involve risk management so that risks can be identified and remediated early in the development process.
	Are existing systems regularly assessed against new risks?		The threat environment is dynamic. As new risks become apparent, the mitigations for existing systems should be reviewed
	Are all staff members kept informed about new and changing risks?		Informing staff about new and emerging risks helps maintain engagement and keeps security at front of mind.