

## Threat Management

### Introduction

Modern organisations are facing an unprecedented challenge; to provide sophisticated, flexible business systems, whilst ensuring that they can be protected in the face of increasing attack from external sources and “internal” exploitation.

Additionally, with increasing legislative pressures and compliance measures that bite hard financially and at a personal level, the correct safeguards and controls must deliver real “Demonstrable Control”.

As any business leader will tell you, a business is developed by balancing the level of acceptable risk against the benefit or gain to the business. The trick of course is being aware of the risk on a day to day basis and being able to steer, manage or indeed restrict the risk quickly and efficiently.

Not all that long ago, businesses were able to actively restrict the level of interaction on a system basis, with minimal access to communications and limited internet connectivity. Fast-forward, internet connectivity is now considered an essential tool for undertaking the day to day operations of most operational functions.

Email, Web Search, Instant Messaging & Remote Working are every day tools for most of us. Infact, these tools have become the principal means in which we interact with our Clients, Prospects, Suppliers and indeed the media.

Whilst the opportunities and benefits that this mode of operation brings are significant, the level of threat is also magnified. For that reason and not to encumber the real advantages to the business, new risks must be identified and controlled, processes and combative solutions should be introduced to mitigate exposure and policies created and upheld to manage personnel interaction.

### Who Benefits?

A business can be viewed as a living entity with all elements, personnel, systems, capital assets contributing for the greater good of all, achieving goals and targets. The whole is **greater than the sum** of its **parts**.

Anything or anyone that impedes or negatively interrupts this activity creates the potential to damage its essential operating functions or the perceived value, typically: Brand Value, Financial Stability & Credit Rating.

It therefore can be argued that both the business and the individuals are benefactors of threat management, as each are reliant on the other to achieve their mission or safeguard their livelihood. From this standpoint, it is critical that all elements remain productive and must be the focus of the security investment and the basis of a "Return on Investment" (ROI).

### **An Ongoing Business Problem**

To succeed in the warp factor speed of today's business world, if a business wants to thrive and grow, it must be willing to gamble with both its Intellectual Property and its technical resources and expose them to the marketplace. This fact alone although increasing the potential of growth again introduces further threat to the business.

This problem is not limited to just large organisations but to any business or entity that uses modern technology.

Threat management must therefore provide the control mechanisms to be sensing, monitoring, responsive, adaptive and restrictive where needed and to provide a comprehensive audit of all activity.

Security is so aligned with the success or failure in achieving goals and ensuring resiliency, that competency in securing itself has to be paramount to any business.

### **Regulations**

Complying with regulations is certainly an important activity but it cannot replace a strategic and goal focussed security management process. A false sense of security can be fostered purely by being compliant! Assets that are subject to regulation maybe covered but others maybe neglected or left unprotected.

Surely a central approach considering the impact of threats on the business as a whole, reviewing which activities offer the highest risk to the business and which processes or practices require attention, has to be how to focus on real security requirements and what is best for the organisation.

## Conclusion

Threat management is an area which cannot continue to be approached purely via a technology basis and requires the mindset of both technologist and business leaders.

As we have established, for a business to develop risks have to be taken but with a real understanding of the threat to the organisation. Personnel need to have the ability to use all of the technology available for the benefit of the business and to meet their targets.

The business also needs to be confident that the resources are being used in a professional and business like approach and in the manner that they were intended. Not as a tool to self harm the business or drain valuable resources.

Clearly as in all business, targets and objectives need to be set determining the benefits that are to be achieved from Security and thereby providing a basis to evaluate the "Return on Investment" (ROI) from the security resources.

Today's approach therefore requires a view of more controlled open assets rather than being "locked down". Organisation will then benefit from being more agile and allow the security resource to contribute to the business goals.

C J Dean  
April 2007

Colin Dean is the Commercial Business Development Manager of Forensic Software Ltd, whose Threat Management solution Policy Central Enterprise (PCE) is used throughout the world in all market sectors.

Contact details:

[Colind@forensicsoftware.co.uk](mailto:Colind@forensicsoftware.co.uk)

Tel: 01483 202990

Mob: 07808 062181