

# » Security Leadership not Security Management «

A white paper by Edward Hamilton,  
Siemens Insight Consulting



Numerous organisations have all the building blocks of effective security but still their employees are not engaged and do not understand what the security department does and why it is needed. "Isn't it just a cost overhead?"

Organisations do not employ security managers and a security department for the sake of having security – the main business driver for any organisation is to make **profit**. Even if they are a non-profit body like a charity they still need to make best use of donations. Subsequent drivers are **legal** and to comply with **regulation**. Any security manager must be aware of this and ensure that the security department assists the business in achieving these goals.

In 1958 Tannenbaum & Schmidt<sup>1</sup> devised a model of leadership behaviours - from

autocratic to democratic. This model consisted of seven levels:

<b>Tell</b>	1	Manager makes the decisions
<b>Sell</b>	2	Manager sells the decisions
<b>Consult</b>	3	Manager presents ideas and invites questions
	4	Manager presents tentative decisions subject to change
	5	Manager presents problem, gets suggestions, makes decision
<b>Share</b>	6	Manager defines limits; asks group to make decisions
	7	Manager permits subordinate to function within limits defined by superior

<sup>1</sup>Tannenbaum and Schmidt (1958) - How to choose a leadership pattern. Harvard Business Review.

When dealing with senior management, the majority of security managers work at the consultative level, but when working and communicating with employees, the majority of security managers are still operating at level 1 – **Tell** – “You shall do .....” Is it any wonder that employees perceive security as a hindrance?

#### **Effective Security**

If security is going to be effective, all the employees from the boardroom to the store room must believe security is essential and perceive it as a benefit. If, as a security manager, we are telling or selling the employees on how their business processes and systems must be secured, we are failing to:

- Secure the business - If an employee perceives security as a barrier they will find ways around the security processes to make their working lives easier – Many of us have seen PCs in hospital wards logged in to all the applications with various staff using the PC without changing user identities
- Engage staff in understanding the impact of security breaches and how this affects the business
- Train staff to be security aware and take a proactive role in security.

Employees that understand the business and security will come up with a balanced approach and they will be more willing to follow the organisation’s policies if they helped to define them in the first place.

#### **Management or Leadership**

The Tannenbaum & Schmidt model is accepted as standard good practice for management. Why are we, as security managers, not taking management best practice and using it to make security one of the key cornerstones of the organisations we work within?

It is very unlikely that, as a security department, we will ever achieve a culture to enable levels 6 and 7 “Share” to be used on a consistent basis. Wouldn’t it be fantastic to have the organisation informing you of an appropriate set of security controls, which meet the organisation’s policies, and all they are asking you to do is approve them?

At board level within most organisations, there is an understanding of risk and risk management. There has been a significant amount of research into how to effectively reduce and mitigate risk throughout an organisation, and the majority of the research into embedding risk management shows the most effective methodology is to create a risk culture. As security is a subset of risk management, why are security managers not trying to embed a security culture within their organisations?

#### **Benefits to the Organisation**

Developing a healthy security culture takes time and progress is extremely difficult to measure. I have been in meetings where the director responsible for security was complaining that they had invested a lot of money in incident management. However, since that time, the number of incidents had increased. He could not understand that making employees aware of the types of security incidents and reporting mechanisms would, inevitably, lead to more incidents being reported.

There are no easy ways to demonstrate the benefits of engaging with employees regarding security. As a security manager, you will not have a nice pile of policies or equipment racks full of security appliances that can be shown to senior management and the auditors. Most security managers are constantly battling and fire-fighting to get the most basic controls in place with every single project and department. With cultural change it will allow you to concentrate on the next threats and issues and ensure your organisation is prepared for them. It will take time, but over a period, your role as security manager will change as the core corporate security principles are embedded throughout the organisation from day-to-day security management to one of corporate governance and leadership.

Bolton and Blackburn<sup>2</sup> identified eight benefits of embedding risk management within an organisation:

1. Reduction in management time spent firefighting
2. Fewer sudden shocks and unwelcome surprises
3. More focus internally on doing the right thing in the right way, therefore:
4. More likelihood of achieving business objectives
5. More likelihood of implementing change initiatives
6. Strategy being appraised more effectively
7. More confidence in moving into new areas
8. Overall costs of risk are reduced.

If, as Security Manager, you can achieve the benefits listed above, it would have a significant positive impact on your organisation.

As employees become more security aware, they will start to report security concerns and incidents. These concerns and incidents will increase to a peak, until the culture grows and the employees take greater ownership. Once the culture is matured, the level of incidents and the amount of resources required to manage them will decrease.

---

<sup>2</sup> Bolton and Blackburn (2002) – Embedding Risk Management May 2002, Housing Corporation

# Security Leadership not Security Management

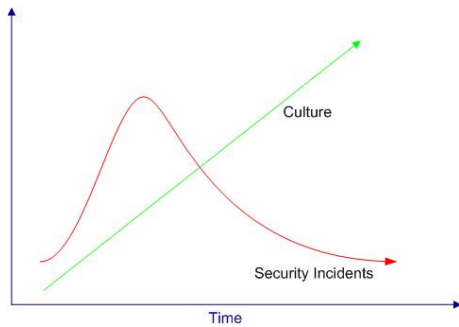


Figure 1-Culture vs Security Incidents

For example – in the 1970's drink-driving was accepted. You might get caught by the police, but like speeding today, it was generally acknowledged that everybody did it occasionally. Now drink-driving is socially unacceptable. The increased awareness of the risks and potential repercussions of drink-driving has led to those who may have previously flaunted the law to now discourage others from doing so. It took a lot of work by the government and police to change the culture within the UK, but in the long-term, changing the culture is more effective and cost efficient.

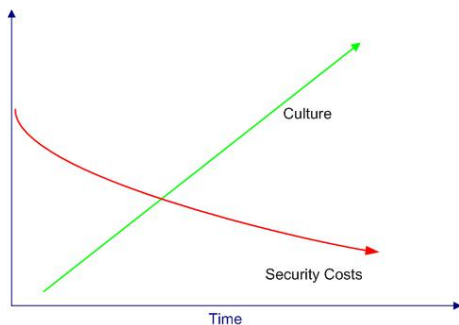


Figure 2-Culture vs Security Expenditure

## Developing a Security Culture

Developing a security culture is like developing any other type of culture within an organisation, and, again, there has been significant research on the subject. Robbins and Smith developed a model of seven organisational areas that are closely interlinked with culture:

1. Style of decision making
2. Objectives
3. Competitive advantage
4. Organisational structure

5. Management systems
  6. Management of people
  7. Functional strategies and policies
- Information systems.

As the person responsible for security within your organisation, you are significantly empowered to define and/or influence how your organisation manages the seven areas specified above, allowing you to define the most appropriate strategies and enabling you to create an effective security culture.

In summary, to enable security leadership, you must:

1. Consult with the whole organisation, not just the board
2. Provide a security framework for the organisation to build upon
3. Raise awareness of the legal, regulatory mandates and the impact security breaches have to the organisation
4. Encourage feedback and positive communication
5. Make security an enabler to the organisation, not a barrier.

As security managers, we need to understand that there is more to security management than just security and management – the essential role that we must be aspiring to is **leadership in the area of security governance** – providing your organisation with the leadership and strategy to secure the organisation, with security as a business enabler, assisting the business in meeting its core goals and be prepared for the security risks of the future.

If you would like further information or to discuss this topics raised within this white paper, please feel free to contact Edward Hamilton via [insight@insight.co.uk](mailto:insight@insight.co.uk) or phone 01932 241000.

## Bibliography

Tannenbaum and Schmidt (1958) - How to choose a leadership pattern, Harvard Business Review

Bolton and Blackburn (2002) – Embedding Risk Management May 2002, Housing Corporation

Robbins and Smith (2000) – Managing risk for corporate governance, BSI.



## Author's biography

**Edward Hamilton** is Head of Operations at Insight Consulting. He has over 15 years Information Technology experience, of which 10 years has been spent specialising in Information Security. He holds an upper second BSc (Hons) in Computer Science

Edward's particular specialist arena is in the design, implementation and management of secure network infrastructures, this includes:

- Managing complex technical projects to ensure they are delivered to time and on budget, whilst ensuring the security of the organisation is not compromised
- Network perimeter security solutions including firewalls, remote access, e-mail and web content checking
- Remote access and site to site Virtual Private Networks (VPN's) solutions utilising various vendor solutions, including VPN solutions that are compliant with HMG manual V
- Authentication solutions using various token and smartcard products
- Delivering solutions to organisations which leverage technology to meet their business requirements while ensuring the solution is appropriate, cost effective and compliant to the necessary standards
- Working with IT Security Teams and Project managers to ensure that projects provided by third party suppliers and outsourcers are cost effective, meet the client business requirements and are secure
- Undertaking and managing IT health checks, network vulnerability and penetration testing.

Insight Consulting is the specialist Security, Compliance, Continuity and Identity Management unit of Siemens Communications and offers a complete, end-to-end portfolio encompassing:

- Security
- Continuity
- Managed Services
- Compliance
- Identity Management
- Training

Siemens Insight Consulting subscribes to the CESG Listed Advisor Scheme (CLAS) and CHECK services. We're also certified against BS 7799 and are a preferred supplier of services to the UK Government and are an accredited Catalyst supplier.

If you'd like to find out more about how we can help you manage risk in your organisation, visit our web site at [www.siemens.co.uk/insight](http://www.siemens.co.uk/insight)  
 Siemens Insight Consulting  
 Tel: +44 (0)1932 241000  
 Fax: +44 (0)1932 236868

[www.siemens.co.uk/insight](http://www.siemens.co.uk/insight)