WHEN A SECURITY POLICY MATURES INTO A SECURITY SOLUTION…

Do you have a security policy?
Yes

Can I see your security policy?
Yes, off course!

When last was this policy updated?
Mmm, not quite sure … but it could not have been ***that*** *long ago…*

How do you distribute the policy to the current employees and new employees?
O, we are very proud to say that we have an excellent Intranet where we have a dedicated link to our library of policies, standards and procedures. All current and new employees know how to access and use the Intranet.

How are you guaranteed that the employees will use this link and will actually read the policy, apply the standard and follow the procedures? Do they sign a legal contract ensuring they are aware of their roles and responsibilities in terms of Information Security?
As I said, the documents are on the Intranet…

Do you have a security officer who ensures that the latest system vulnerabilities are researched, the latest patches installed that the system is systematically upgraded to the latest version, adequate access controls are in place and that password policies are implemented?
I'm sure they know what they're doing. Computers are like a hobby for most of these guys.

What auditing and logging rules are applied to your system?
The system administrators know the users on their systems, they don't need excessive auditing and logging features activated. Besides, do you have any idea how these auditing tools slow down system performance?

What are the current backup procedures?
We have daily weekly, monthly and yearly backups. We send the types on a monthly basis to an off-site backup facility.

Have you tested the types?
Why? Are you saying we are using faulty backup equipment!

What are your Disaster Recovery procedures?
It is on the Intranet.
What if the Intranet can not be accessed?
Thank you for your time.

WHAT HAPPENED TO ALL THOSE SECURITY POLICIES?

It is quite common that companies go through the lengthy process of hiring consultants to develop every information security policy that exists and then… place them on the Intranet!

It is as if the soul purpose of this policy became to satisfy the auditing bodies. This must be one of the reasons why business employees and IT personnel do not perceive policies generally that positively. As employees join, they find it in their 'new employee starter pack' and are pressured to fill and sign the forms ASAP, as HR need to complete their personnel file. IT staff are supposed to use the policies in their daily activities but policies are out of date and does not apply to the newest releases.

It is difficult to determine what is worse, no policy or an out of date copy. A paper written by Control Data Systems stated:

"…security breaches are linked to common weaknesses in the security policy… accidents waiting to happen."

It seems like the success recipe does not lie in how brilliant and on-the-spot the policy is written, but how well the human element is managed in the process of making 'them' use it! It is as simple as, ignore the human and you wasted your time and money compiling it.

WHEN DOES A POLICY 'FAIL'?

1. *When the employee thinks it is a 'stupid' policy.*

A security policy will be used when an employee wants to ensure that the system is appropriately protected. BUT, what if the employee is not aware that the system needs protection? If they don't see the need for the policy they will not include the usage thereof in their daily activities.

2. *When management thinks it is a 'stupid policy.*

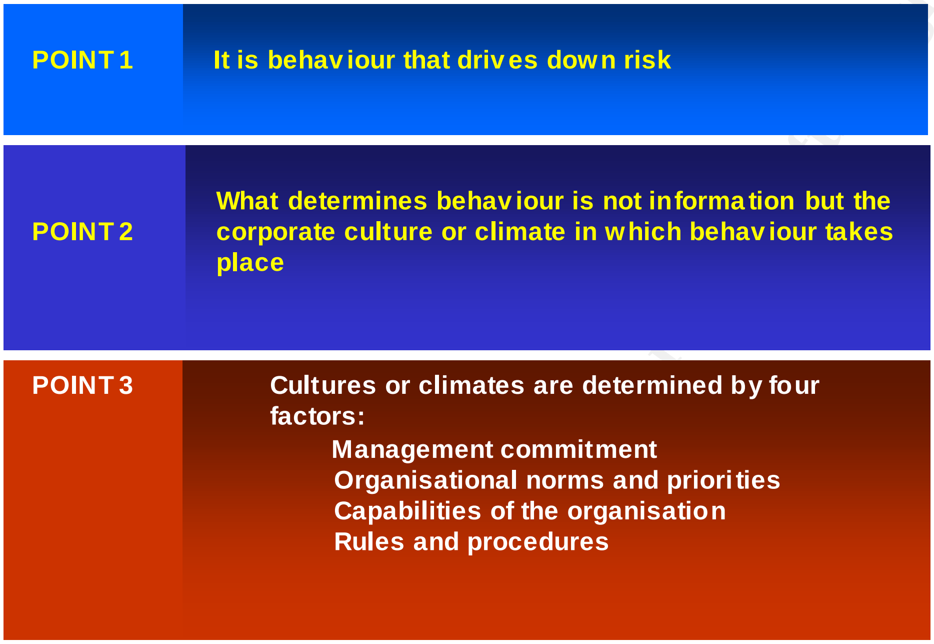
Learn by example…

An employee's behavior will depend on the company's culture. A manager who does not understand the need for the policy will not allocate budget, time or control procedures to bring the policy in existence or keep it in existence. It is more pulling the success of the policy from the top, than to try and push the idea from the bottom.

For people to practice good security, management must provide direction and set the example.

In order for management to set the example they must take responsibility for the security of their information. In this way management will ensure that people practice good security in the area that the manager is responsible for.

The following diagram from the Information Security Forum, illustrates the relationship between the organisation's culture influencing the employee's behavior.



POINT 1

It is behaviour that drives down risk

POINT 2

What determines behaviour is not information but the corporate culture or climate in which behaviour takes place

POINT 3

Cultures or climates are determined by four factors:

Management commitment
Organisational norms and priorities
Capabilities of the organisation
Rules and procedures

Figure1: Corporate culture and climate: What drives down risk?

3. *When the policy has not been tested.*

To know if a policy is really going to qualify as being a solution, it must be 'used'. How many policies get only to be tested after an emergency occurred - which might be too late? Control Data Systems wrote:

> "*Don't expect to perfect your policy and go home. Security is a 24-hour job…it's never finished*"

4. *The policy is not customized for the business environment.*

If 100 % security was practically possible it still might not always be the goal.

The policy must be designed and created around the business culture where it has to be implemented. Employees will not use a policy that makes life more difficult even though the policy might ensure a very secure environment when followed step by step. A policy must pass the test of time. If it failed, the reason must be identified and the policy must be changed accordingly.

5. *The workflow procedures were not practical.*

The policy is perfect. The people accept it. The daily workflow rejects it.

This I see as the most important and most challenging step. You need to understand how the company's business processes gel together and how your policy is going to encourage a symbiotic relationship between people and process. If the daily cycle rejects the process the reason might be one or a combination of the following reasons:

- The level of security was unnecessary high, making the security process too tedious (the criticality of the system did not justify the security effort).
- The involved parties were not aware of how these procedures were going to protect company assets. Shortcuts were taken - bypassing the security policy.

WHAT SHOULD YOU DO TO PROLONG THE EXISTENCE AND INCREASE THE USAGE OF A SECURITY POLICY?

In short:

1. *Plan the goal of the policy by asking:*
   - What should this policy achieve?
   - Will this policy reduce risk?
   - Who is the audience?
   - What is the business culture?

2. *Support the policy with a security awareness campaign.*
   If the users of the policy understand the security risk and how this policy can reduce business risk, the chances of users excepting and using the police increases. Once the policy has been developed, proper change management procedures should be followed. This includes awareness presentations to the users who will be effected by the implementation of the policy. Users usually do not like surprises. For example, to logon to their system, as any other day, and then being prompted with the message of their password, which is going to expire after another 10 attempts, might bring confusion and misinterpretations. The message could be ignored and employees are locked out of the system. Or they choose a new password and for the first time they are not allowed to use a previous password, their chosen password is too short or their chosen password does not contain a mixture of numbers, letters and special characters. Just enough to drive user and system administrator to a point where bypassing the policy are somehow now justified…

3. *Check if the policies are enforced.*
   Sometimes it is not the policy and the implementation procedures, which failed, but the user who have an indifferent attitude towards using the policy. It is then necessary to enforce users to use the policies. Management can even consider adding this criteria to the employee performance contracts in other words measuring work performance against how well the employee adhered to company policies.

Policies also need to be re-evaluated regularly to ensure that it is not out of date. According to studies done by a marketing company, *Datamonitor*, 70 % of companies are not aware of how often their policies are revised. They wrote:

> *"… 250 companies across 5 key vertical sectors in Europe = 75% of enterprises surveyed claim to have a clearly defined security policy. However, paradoxically, some 70% of those interviewed do not know when, or how often, the policy is revised.*

4. *Check if the policies are applicable.*
How do you know how many policies a company needs? Where do you stop developing them?

If you don't know where you are heading you won't now where to stop. Developing policies and procedures could be a livelong exercise. Ever used a search engine for tracing documents to "policies and procedures"? There are quite a lot of choices and one tends to panic and think - where do you actually stop developing and implementing? The answer lies in performing a proper technical vulnerability assessment exercise and together with best practices guidelines, identify the needed solutions.

The vulnerability assessment results will be able to give you a clear indication of whether:

- security standards were used during implementation of the system
- the security administrator is performing standard maintenance functions
- the system is securely configured.

This will help identifying which policies, standards and procedures will be targeted as an starting point. Policies should not just be developed in an unstructured way. Use a standard that will help you to address these identified 'problem' areas in a structured way.

One such standard is the British Standard 7799 (BS7799).

> *"BS 7799 is intended to serve as a single reference point for identifying a range of controls needed for most situations where information systems are used in industry and commerce, and to be used by large, medium and small organizations."*

A company can also decide to be compliant to this international standard and will be audited regularly to keep or acquire their certification status. BS7799 is a standard to which companies can benchmark themselves. This standard divides a company in different information security control areas and sub-areas. The technical vulnerability results and the BS7799 security control areas form a framework to identify needed policies in a structured way. This way you are ensuring that you address the important security areas, thus knowing where to start and knowing where to end.

5. *Perform post-implementation testing.*
   How do you know if the policies are 'working'?

   The policies were chosen, because security vulnerabilities were found on the system. The policy will be successful if the security vulnerabilities were reduced to a suitable level. If the security exposure was not reduced, the policy was failing its purpose and should be changed accordingly.

CONCLUSION

An organisation needs security policies, standards and procedures to enforce information security in a structured and thorough way. The choice of policies needed by the organisation should be acquired through a proper risk analysis, which includes technical vulnerability assessments. The results together with a proper policy framework should determine which policies are needed for this specific organisation. Implementation of the chosen policies should be assisted by proper training and awareness courses to clearly indicate how these policies, standards and procedures will effect employee's daily work activities. Post implementation testing should indicate whether the security exposures were reduced. - it is at this stage that one can measure if the ***security policy matured into a security solution.***

REFERENCES

1. Clifford, Richard. "eSecurity - What Security?". November 2000. URL: http://www.datamonitor.com/productdetail.asp?id=dmtc0727&ref=Search%20Results (26 March 2001).

2. CONTROL DATA, "Why security Policies fail". White Paper. 1999. URL: http://www.us.syntegra.com/working/security/m_whitepapers.shtml (26 March 2001)

3. SECURITY POLICY, "BS 7799: Compliance Management made easy ". 2000. URL: http://www.ca-systems.zetnet.co.uk/bs7799/index.htm (26March 2001).

4. SECURITY POLICY, "Applying Information Security Policies & Computer Security Standards". 2000. URL: http://www.securitypolicy.co.uk/secpolicy/ (26 March 2001)

5. Information Security Forum (ISF), "Driving Information Risk out of Business". April 1999.

RESOURCES:

1.

70% of companies do not know when or how often their security policy is revised
eSecurity breaches cause over US $15 billion damage worldwide annually yet a European report published by leading market analysis firm Datamonitor reveals that a remarkable 70% of companies do not know when, or how often, their IT security policy is revised.
According to the report, **eSecurity - what security?** , which surveyed decision-makers in over 250 companies across 5 key vertical sectors in Europe, 75% of enterprises surveyed claim to have a clearly defined security policy. However, paradoxically, some 70% of those interviewed do not know when, or how often, the policy is revised. This indicates that the majority of the respondents do not have a firm grasp of what constitutes a security policy. Despite numerous high profile attacks, companies are still not taking eSecurity seriously.
Datamonitor analyst Richard Clifford comments:

"Just because a company has passwords to authenticate their users, anti-virus software and firewalls does not necessarily mean that there is a security policy in place. It is likely that respondents that do not know when their policy is revised in fact do not have one in place. When businesses become aware of the risks that are inherent to eBusiness and have implemented advanced security systems to protect themselves, clearly defined policies will be a necessity."
A security policy is highly dependent on enforcement. Many of the companies use basic security products that do not require policy enforcement. Passwords, anti-virus and firewalls are stand-alone products that do not require policy management to ensure that they are working effectively.
That 70% answered that they did not know when, or how often, their security policy is revised, indicates either an ignorance about security or, perhaps more worryingly, a lack of it.

2. <see mail attachment>

3.

BS 7799:
COMPLIANCE MANAGEMENT
MADE EASY

BS7799 Consultant: The BS 7799 Product

*** NEW: Product download now available ***

BS 7799, first published in February 1995, is a comprehensive set of controls comprising best practices in information security. BS 7799 is intended to serve as a single reference point for identifying a range of controls needed for most situations where information systems are used in industry and commerce, and to be used by large, medium and small organizations. It was significantly revised and improved in May 1999.
With BS 7799 accreditation and certification schemes firmly in place, BS 7799 may ultimately become a benchmark against which all companies will be measured. There have even been suggestions of mandatory inclusion of an organization's BS7799 status within its annual returns/report.

4.

Applying Information Security Policies & Computer Security

Standards

Easier Implementation Of Your Security Policies

Security policies, information security standards, computer security standards, information security policies, computer security policies, baseline security policies... words that present a headache to so many organizations!

Information security policies and computer security standards must be implemented to be effective. **But how can this be achieved in a large organization? How can the task be effectively managed and monitored?**

5. <see mail attachment>