CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Making Information Security Policy Happen

Key Message: Targeted, innovative communications and a robust life cycle are keys for security policy success.

Executive Summary

When done well, security policy sets the tone and direction for how the organization will protect its critical information assets. An effective policy life cycle starts with a credible, well-defined foundation, actively engages key stakeholders, includes a policy exception process, requires regular policy review and update, uses innovative and targeted forms of communication, and calls for tracking and reporting key performance measures.

In this podcast, Paul Love, Director of Information Security for The Standard, discusses how to put an information security (IS) program in place that reflects management's intent – and gets users on-board and engaged.

PART 1: KNOW YOUR REQUIREMENTS; MAKE SURE BUSINESS LEADERS ARE ENGAGEDM

Why Security Policy Is Critical

Security policies are generally viewed as an underdog or necessary evil.

Security policy, determined by senior management, sets the tone for the entire IS program. In effect policy serves as their voice to the organization on expected minimum requirements.

A clear statement of policy allows management to own this. It then allows the CISO and his or her staff to serve as consultants to the organization instead of being viewed as the ones trying to drive the program.

Sources of Security Policy Requirements

Policy requirements derive from:

- Regulatory, contractual, and legal requirements
- Business requirements
- Internationally recognized standards such as the ISO 27000 series, ISO 27001 and ISO 27002 (previously ISO 17799) in particular

It is easier to start with a well-recognized, vetted standard than with selecting topics from scratch. Using such a source lends credibility to the initial set of topics you select.

One cautionary note: You need to make sure that any standards you use as a starting point match your business needs and regulatory requirements.

Tailoring is accomplished by close collaboration with key stakeholders in the organization, such as your legal office.

A Business Leader's Role and Responsibilities

Business leaders are responsible for:

- making sure their staff members fully understand the requirements they are expected to fulfill based on their roles

- modeling the behavior that they want staff to emulate
- providing visible, active, day-to-day support for the organization's objectives and policies
- acting promptly when seeing deviations from policies and supporting processes. Ensuring that such behavior is identified, corrected, and reported.
    - Do not do this in a punitive way. Reinforce expected behavior.

As the CISO or Director of IS, focus on the people and process aspects of IS policy by:

- walking around and talking to people about policy, and ensuring they understand why it is important.
- working with other business leaders to make sure they are working with their teams.

While discussing policy during annual planning processes or during performance reviews may be helpful, it works better if security is not specifically called out or highlighted. It should be treated as part of corporate values, part of day-to-day business and the right thing to do – versus being treated as an event.

PART 2: POLICY STRUCTURE AND LIFE CYCLE

Policy Structure: Procedures, Standards, and Guidelines

When developing a policy structure, it is important to target the right document to the right internal customer and break each topic into digestible chunks.

Policy at the highest level should be short, concise, and have a lengthy shelf life. It is a simple statement from management of their intent, stating the top-level control objective.

- For example, "Information in transit or rest will be encrypted to prevent disclosure to unauthorized parties."

Such statements need to be technology-independent given how rapidly technology changes.

Standards spell out the compulsory, actionable requirements that support policies. Standards are generally used by the IS team and other subject matter experts.

- In the example above, the corresponding standard would address specific types of encryption such as AES (Advanced Encryption Standard).

Guidelines are generally non-compulsory best practice recommendations, provided for cases where there is a need to exceed minimum requirements.

Procedures provide step-by-step implementation instructions. They are very detailed, prescriptive, and technology-dependent. Procedures are expected to change frequently.

- In the encryption example, a procedure would state "Install software on this system. Press the start button. Move here and enter this information." And so forth.

Security Policy Life Cycle

An effective security policy life cycle includes the following process steps:

1. Start with your existing policies if they are current and reflect management's intent. Identify the gaps between your policy and an industry-recognized standard such as ISO 27001.
2. Communicate often and in various ways with those affected by the policy and those who will approve the policy.
3. Understand and articulate the risks associated with both implementing and NOT implementing the policy, to help business leaders make well-informed decisions.
4. Describe the role that the IS department should have with respect to policy and the policy life cycle. Being an

advisor or consultant to the business is most effective for building a trust relationship.
5. The organization's risk tolerance is defined by the policy and driven by business needs. Keep this in mind as you develop policy language.
6. Make sure you have a process for continuous review and updating of policies. This is best done on a scheduled basis – every six months is a good time frame. Policy review and update should also occur when business conditions or technologies change.

Make sure you have defined a policy exception process. This is often overlooked but is critical due to changing business conditions and regulatory requirements.

At the end of the year, present policy exceptions to management so they can determine if such exceptions call for a change in policy.

PART 3: ENGAGE USERS AND TRACK POLICY PERFORMANCE

Keep Users Current on Their Policy Responsibilities

While email and other forms of passive communication have their place, communication about policy needs to be constant, relevant, and engaging.

One recommendation is to conduct training that describes how users should protect themselves and their personal information at home – something that they care about. This is easy for people to understand and grab on to.

Generally people who implement practices at home will transfer these habits into their work environment.

Another effective awareness-raising approach is to create digests of specific policy information that are relevant for specific roles – such as system administrators, software developers, and remote employees.

Supplement this information with banner ads on your internal website, annual online multi-media training, and targeted emails with interesting messages.

Measure Policy Effectiveness

As CISO or Director of IS, you need to understand (i) where deviations from policy are occurring and (ii) the root cause for the deviations. For example:

- Did the end user know about the policy?
- Did they decide not to follow it?
- Did their management support them not following the policy?

Another useful measure is tracking the number and type of policy exceptions, and which exceptions were approved by management.

A less tangible, but no less useful, measure is tracking how often users seek your advice, offer suggestions, and ask for policy interpretations.

Resources

CERT, in particular CERT's governance portal and CERT's Virtual Training Environment (search on "policy")

SANS Security Policy Project

ISO 27000 series