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

Concrete Steps for Implementing an Information Security Program

Key Message: A sustainable security program is based on business-aligned strategy, policy, awareness, implementation, monitoring, and remediation.

Executive Summary

Most security leaders understand the necessity for strong tone at the top and a designated executive champion if a security program is to have any chance of success. But once these are in place, it is essential to create an effective program that aligns with changing business objectives and has a well-articulated strategy that is implemented through policy and regularly monitored for compliance. A sustainable program relies heavily on well-defined measures and automation.

In this podcast, Jennifer Bayuk, an information security specialist and former Chief Information Security Officer at Bear Stearns, discusses the necessary steps to create an information security (IS) program that has these characteristics, based on her book *Stepping Through the InfoSec Program* [Bayuk 2007].

PART 1: LEADERSHIP ROLES AND ALIGNING WITH BUSINESS STRATEGY

Roles in the Best Position to Champion a Strong IS Program

Any role with control over technology is in a great position to serve as IS program champion. This includes the CIO (Chief Information Officer) and the COO (Chief Operating Officer).

The CEO is the best catalyst for setting the tone at the top, reinforcing the value of information protection and privacy. For example, if the CEO states that employee information is to be protected, Human Resources can develop an awareness and information protection program that staff is likely to follow.

Roles such as the Chief Risk Officer or Internal Audit can be effective champions given the right tone at the top. Typically these roles do not control resources directly so they may have difficulty if not teamed with a role that directly controls and influences information technology.

Making Sure the Security Program Supports the Business

Business alignment comes with recognizing the information assets and technology processes that are key to accomplishing business objectives.

Security leaders need to understand how the business operates, what information it uses, and the data flow and systems that are involved in achieving day-to-day objectives.

Risk management is key for getting senior leadership attention, ensuring that IS risks are described in terms that business leaders understand. Examples include intellectual property falling into the hands of competitors and theft of customer identities.

Step 1: Strategy

With this understanding, security leaders are then able to devise and implement a security strategy and policies that reflect business objectives.

PART 2: BUILDING ON STRATEGY, THE FIVE KEY COMPONENTS OF AN IS PROGRAM

Step 2: Policy

Security policy documents an agreed-upon set of mandates, authorized by the IS program champion, reflecting the tone at the top.

Step 3: Awareness

To enact policy, you need to have an effective awareness program. Awareness includes outreach and training that clearly convey staff roles and responsibilities.

Staff members need to understand that security is a personal job responsibility for everyone in the organization.

Role-based awareness and training are essential. Examples include targeted training for system administrators, users of a particular application or business process, and those who staff the help desk. All roles need to understand the balance between protecting information and having access to that information. In addition, all roles need to have the appropriate level of authority to fulfill their responsibilities.

Steps 4 and 5: Implementation and Monitoring

If Steps 1, 2, and 3 are performed correctly, implementation is fairly straightforward and aligned with the IS strategy.

This is where automation can be helpful in ensuring that implementation is in line with management objectives.

Self-Assessment

While self-assessment, or an internal audit, can be viewed as a type of monitoring, typically these methods are used prior to implementation to raise awareness and help demonstrate that the planned implementation will be effective.

Monitoring, as discussed here, is targeted on real-time monitoring of actual system and software configurations. Monitoring is the feedback loop to make sure that what you thought you were implementing is indeed in place and reflects policy.

Monitoring intends to demonstrate that security controls have been implemented in accordance with management objectives – that the IS program is doing the right thing and producing the right outcome. This is sometimes confused with asking “Did we follow the right process?” which is necessary but not sufficient.

Step 6: Remediation

Remediation is triggered when monitoring identifies an error or omission that needs to be addressed. Sometimes processes are correctly followed but still produce an inaccurate result. This then requires a change to the process.

Inputs to remediation include feedback from monitoring all of the other steps: awareness, implementation, policy, and strategy.

Remediation can recommend changes to procedures and security measures all the way to a complete change of organizational structure. The latter may result from not having the right authority, the right management buy-in, or the right business alignment.

Remediation completes the continuous improvement and feedback loop for the security program to ensure it is in sync with business objectives.

PART 3: MEASUREMENT AND AUTOMATION

Different Measurement Strategies for Different Objectives

One type of measure is based on a pre-established, set target (such as 100% coverage for an identity management system) and then measuring, for example, the extent to which every user, every operating system, and every application reflects the target.

A second type of measure is focused more on the process of interest, such as the remediation or the implementation process, and how effective a process is in getting you to your desired target or outcome.

Measurement Example: Using Process Metrics to Get to Target Metrics

One example is a configuration metric for determining the extent to which the firewall rule set reflects policy. Firewall rules change frequently so you can't just say "this is the correct configuration."

The questions to ask are "What is the process by which the firewall rules change and how do I know that the change is accurate?" This calls for a change control authorization process that is correctly executed.

So, in this case, the monitoring metrics are a representation that:

- All firewall configurations are monitored
- All changes to firewall configurations are automatically detected and reported
- All identified changes are validated as having been authorized in accordance with the change management process

Monitoring metrics represent the execution of the process that, in the end, is meant to give you a target metric – that the firewall rule set reflects policy.

Metrics provide confidence that the IS program is working properly. An assessment or an internal audit provide the overall sanity check that the confidence is deserved.

Where Automation Can Help – and Where Not

Automation works particularly well for areas that are black and white – in cases where you can determine in advance what constitutes a positive or correct outcome (such as change detection).

Automation does not work well where human oversight or subjective decision making is part of the program, such as using a checklist to determine if your vendor's security practices meet your requirements. Checklists that are filled out by people based on subjective judgment do not lend themselves to meaningful automation.

Resources

[Bayuk 2007] Bayuk, Jennifer. *Stepping Through the InfoSec Program*. Information Systems Audit and Control Association (ISACA), 2007.

Bayuk 2008] Bayuk, Jennifer. "Good Governance: How to be a Security Leader." Podcast and transcript, BankInfo Security, September 4, 2008. [Requires free registration to access.]

COBIT (Control Objectives for Information and Related Technology), ISACA (Information Systems Audit and Control Association).

Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition. IT Governance Institute, 2006.

ITIL (Information Technology Infrastructure Library)