CERT PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Compliance vs. True Buy-In

Key Message: Integrating security into standard business operating processes and procedures is more effective than treating security as a compliance exercise. Leaders must lead by example to build and sustain a culture of security.

Executive Summary

Demonstrating compliance with the increasing number of domestic and international laws and regulations is a daunting undertaking if this is tackled one regulation at a time. Organizations that have implemented a living set of standard operating processes and procedures (SOP) find that a small team can generally trace any new external requirement to their SOP. This typically produces a set of manageable changes, many of which result in minimal to no impact to the rest of the organization.

An SOP typically includes well defined roles and responsibilities, commitments and accountabilities; policies and procedures; business process definitions; controls; regular monitoring and reporting; and training and awareness.

Thus compliance is an outcome of good business practice, not a focus for special task teams or projects.

Security as Compliance Checklist vs. Security as Cultural Norm

- Many organizations have spent millions of dollars to comply with Sarbanes-Oxley, in terms of their own actions and those of their internal and external auditors to determine compliance. Each new regulation creates a new "compliance" project with the companion flurry of activity.
- Leading organizations do not experience this
- One of the key differences is the presence of a defined, standard way of doing business; the development and use of standard business processes and operating procedures (SOP) based on objectives and critical success factors, supported by regular review and update
  - Explicit traceability between business objectives, success factors, policies, processes -- an integrated whole
- Compliance with any new regulation then becomes an exercise of mapping the new requirements to the existing SOP, making changes where necessary, often only visible to the team responsible for process improvement
- Compliance quickly becomes business as usual, not the central focus
- The key motivator for security action is a good business reason supported by facts and data. That said, without compliance, it's hard to sustain executive-level attention.

What Steps Can an Organization Take To Get Started?

- Learn from marketplace peers; benchmark
- Not a quick fix; years in the making
- Concentrating on what is core to the business. For example, considering security, what are the organization's key and most critical information assets? Key business processes? Key services? And where are these most at risk?
- Construct a modest set of core business process definitions, standards, policies, and practices
- Use regulatory compliance events (such as Sarbanes-Oxley) as a catalyst, a jumpstart for true, sustainable improvement, not just a checklist exercise
  - Improve internal controls, perform meaningful data capture, define new processes, improve existing ones; focus on repeatability in future years
- Institute a security awareness and training program for new employees and as an ongoing, required refresher for current staff. Measure awareness on a regular basis as part of standard reporting processes.

How Do I Make Buy-In an Enterprise-Wide Practice, a Cultural Norm?

- This is the same question for any type of substantive organizational change (new markets, new products, new competencies)
- Changing human behavior is a tough issue; generally, people are successful because they've done things in a particular way that works for them, so why change?
- Define the benefit and make it personal based on role, so staff can identify their contribution
- Imbue awareness and training with specific examples (we need greater protection for this customer data, so your authentication and access control actions are going to be more painstaking, but here's why)
- Make sure staff understands why the change is important to the business
- Small, constructive actions start to create some cultural momentum and shift
- Alternatively, start with a small group responsible for specific critical processes and controls
    - Work intensively, achieve short-term improvement, make results visible, create pull from other groups
- Over time, work to build a culture of security

An Example

Rhonda MacLean, (former) chief information security officer, Bank of America, describes the bank's approach to enterprise security at both a governance and management level as follows [McCollum 04]:

> On a structural level, Bank of America has established a security compliance framework that includes commitment and accountability, policies and procedures, controls and supervision, regulatory oversight, monitoring, training and awareness, and reporting. Bank of America has also established a four-level information security governance model that maps out the responsibilities of board directors, business executives, chief information officers, corporate audit, the security department, legal, corporate and line-of-business privacy, and supply chain management.
>
> The board of directors is responsible for reviewing the corporate information security program and policy, while senior management is accountable for ensuring compliance with applicable laws, regulations, and guidelines and for establishing compliance roles, accountabilities, performance expectations, and metrics. It's up to the auditors to ensure the commitment and accountability for information security controls.
>
> Bank of America's corporate information security department focuses on people, technology, and processes using a protect/detect/respond-recover model and measures its progress based on the Six Sigma quality methodology. Bank of America measures security based on failed customer interactions rather than on downtime, performance, or the number of infections or attacks. Achieving 99 percent uptime isn't important if the one percent downtime impacts 30 million customers.

References

Allen, Julia. "Governing for Enterprise Security." (CMU/SEI-2005-TN-023). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, June 2005. http://www.sei.cmu.edu/library/abstracts/reports/05tn023.cfm.

Crawford, Michael. "Can compliance be a selling point?" *Computerworld*, March 30, 2006. http://www.computerworld.com.au/index.php/id;1716314144;fp;16;fpid;0

> "The first Australian bank or financial institution to crack the compliance and governance code could profit handsomely from the hard work. Unisys predicts the first financial organization that can realistically tick all the boxes in relation to governance and compliance will be in a position to offer security as a 'value-added' service to competitors in the banking industry."

[Ernst 04] Ernst & Young. "Global Information Security Survey 2004." Available at http://www.ey.com/global/download.nsf/UK/Survey_-_Global_Information_Security_04/$file/EY_GISS_%202004_EYG.pdf.

> Ernst & Young's 2004 Global Information Security Survey states [Ernst 04]:

> "Ultimately, information security is a human enterprise, as demonstrated by respondents citing 'lack of security awareness by users' as the top obstacle to effective information security. No amount of technology can reduce the overriding impact of human complexities, inconsistencies, and peculiarities. Any strategy that overlooks this realization is inherently flawed. With proper training and education, people can become the most effective layer in an organization's defense-in-depth strategy. The first step is making sure they operate in a *security conscious culture*." [italics added]

[McCollum 04] McCollum, Tim. "MacLean: Auditors Play Key Role Against IT Threats." IT Audit 7. Institute of Internal Auditors, May 2004. http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5514.

The SEI's IDEAL^{SM} model for organizational improvement and change: http://www.sei.cmu.edu/ideal/. IDEAL is a service mark of Carnegie Mellon University.