CERT PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Why Business Leaders Should Care About Security

Key Message: This podcast examines why lack of management attention to security can cost an organization millions. Leaders need to be security conscious and to treat adequate security as a non-negotiable requirement of being in business.

Executive Summary

Security's days as just a technical issue are done. It is becoming a central concern for leaders at the highest level of many organizations and governments, transcending national borders. Customers are demanding it as worries about privacy and identity theft grow. Business partners, suppliers, and vendors are requiring it from one another, particularly when providing mutual network and information access. Networked efforts to steal competitive intelligence and engage in extortion are becoming more prevalent. Security breaches are increasingly motivated by financial gain.

This podcast is intended to motivate leaders to pay attention to enterprise and information security, and the risks of not doing so. It introduces two landmark examples of organizations that did not treat adequate security as a high priority. It places security in a governance context and introduces how security can be viewed as a competitive advantage. It discusses creating a culture of security, demonstrating duty of care, and determining who is ultimately responsible for security. It provides some next steps for taking action.

PART 1: Why Should Business Leaders Care About Security?

What happens

- if your customer data is stolen or disclosed, and this is on the front page of The New York Times or The Washington Post?
- if your customers lose confidence because they've become aware of a security breach involving their personal information?
- when strategic plans, key trade secrets, or intellectual property get into the hands of your competitors?

- Treat information as a critical asset at risk, like money, trust, and reputation
- Deploy protection strategies for information that are comparable to other enterprise assets
- Treat information security and information protection as a strategic issue, and compliance will naturally follow; viewing security as solely a compliance exercise is neither effective nor sustainable
- Security is not just about risk, loss, or cost avoidance; attention to security can support taking on more risk in a sensible, well-informed manner

Some Recent Cases

ChoicePoint

- March 2005: ChoicePoint security breach compromised personal information of 163,000 people
- First visible case subject to California Senate Bill 1386 requiring consumer notification (landmark case)
- January 2006: settlement of Federal Trade Commission suit
    - $15M (11% of 2005 profit)
    - $19.3M legal expenses and fees
    - $15-20M decision to exit high-risk business lines

ChoicePoint breach sources:
http://www.washingtonpost.com/wp-dyn/articles/A8587-2005Mar4_2.html
http://blogs.washingtonpost.com/securityfix/2006/01/choicepoint_to_pay_15m_for_pri.html
Privacy Rights Clearinghouse presents a chronology of all reported consumer data breaches since the ChoicePoint breach.

Veterans Administration

- May 3, 2006: theft of data for 26.5M veterans (inc. names, SSNs, dates of birth) and 2.2M active duty and reserve personnel (not reported until May 22)
- VA analyst took home sensitive data and his home was burglarized (including laptop and external hard drive with this data)
- A coalition of veterans groups filed a class-action suit against VA, claiming the department did not properly oversee its information
- VA Secretary Jim Nicholson told the House Committee on Veterans Affairs that it could cost taxpayers up to $500 million to prevent and cover potential losses
- The laptop was located on June 29; it appears that no data was accessed
- Trust is hard to build and sustain; easy to lose in an instant

Veterans Administration breach sources:
Chronology of VA breach:
http://www2.csoonline.com/exclusives/column.html?CID=21678&source=csoupdate
Inspector General's report:
http://www.va.gov/oig/51/FY2006rpts/VAOIG-06-02238-163.pdf
informationweek.com:
http://www.informationweek.com/showArticle.jhtml?articleID=188702127

PART 2: Why Is Security a Governance Issue?

Governance Defined

- Historically applied to the financial aspects of managing an organization
- Setting explicit expectations for the organization and making sure these expectations are fulfilled
- Oversight, directing, and controlling
- Setting the right tone at the top
- Establishing cultural norms, ethics, and values; making security a cultural norm
    - Employees understand what is expected of them
    - An organization is the custodian of its customers' (and employees') information

Tying Security to Governance

- Making sure that security clearly maps to and supports the organization's strategy, business goals and objectives, critical success factors, identifying critical information assets
- Making sure security is part of the normal day-to-day business flow, processes, staff meetings, reporting mechanisms (for example, require regular reports of key security incidents -- why they happened, what damage they caused, what has been done to prevent recurrence)
- Getting security into the mainstream of how the organization does business is an act of governance

How Might This Have Helped ChoicePoint?

- If the Board had made clear that the issue was important, the CEO might have put together an incident recovery

plan and reviewed it or rehearsed it in advance, similar to a continuity or disaster recovery exercise. When the incident occurred, key personnel would have been more prepared to respond.
- Leaders would have made sure all aspects of security were integrated, including information security, physical security, legal, human resources with respect to conducting background checks of potential clients, audit to ensure appropriate controls in place.
- Governance would have fostered convergence of organizational functions that have a role to play in security.
- Preventive controls would have been established up-front.
- There could have been some potential legal benefit to being able to argue "we addressed the issue in advance and used best known practices."

PART 3: Competitive Advantage, Duty of Care, and Who's Responsible?

Security as a Competitive Advantage

- Global business; global supply chain; 24x7 operations and access to competencies worldwide
- Reputation: recognized as safeguarding and protecting customer information, a good custodian, builds trust
- New business transactions, products, and services
- Effective branding (like Volvo for safety)
- eBay bought PayPal based on customer demand for a secure payment service. Customers know that their financial transactions are protected.

  Additionally:
  - Enabling new types of products and services, and new channels to new markets
  - Communicating with customers in a reliable, cost-effective, and timely manner
  - Allowing transactions to occur with greater integrity and privacy
  - Enabling profitable new types of customer/supplier engagements
  - Providing more secure access by internal and external staff to enterprise applications

Duty of Care

- Duty of care required for governance of digital security
- Based on business judgment rule: The level of care that a reasonably prudent director of a similar organization would have used
- Negligence is failure to do so
- Doing the right thing regardless of a cost incentive

For example, if the majority of organizations in the healthcare sector have included information security in their business continuity plans and exercises, others in this sector are expected to do the same.

Who's Responsible

- Key is bringing all of the involved parties together regularly in an action-based forum
- CEO is ultimately accountable; Board of Directors have a role to play (policy)
- CEO will often delegate next-level responsibility to one or more of: Chief Information Officer, Chief Information Security Officer, Chief Privacy Officer, Chief Risk Officer, or a steering council/committee
- Implementation-level responsibility typically resides with the IT organization and security functions responsible for security processes and controls

In a Nutshell

- Security-conscious leadership; addressing security (or not) as a conscious, informed act

Cultural behavior and norms appropriate to risks and exposures
- Adequate security as a non-negotiable requirement of being in business

Next Steps

- Risk assessment to identify critical information assets and their exposures and risks
- Rank and stack protection strategies necessary to mitigate high-priority risks
- Create management oversight councils
- Measure, measure, measure (for example, Balanced ScoreCard, management dashboards)
- Integrate security measurements with other organizational measurement and reporting processes
- For more information: http://www.cert.org/nav/index_green.html, CERT Governance Portal

Security-Conscious Culture (excerpts from [Allen 05], [DHS 06])

Security must come off the technical sidelines and not be relegated to software development and IT departments. Boards of directors, senior executives, and managers all must work to establish and reinforce a relentless drive toward effective enterprise security. If the responsibility for enterprise security is assigned to someone who lacks the authority, accountability and resources to enforce it, the desired level of security will not be articulated, achieved, or sustained. Even the best efforts to buy secure software and build security into developed software meet "considerable resistance because the problem is mostly organizational and cultural, not technical" [Steven 06].

This shift in perspective elevates security to more than just a standalone technical concern. Because security is now a business problem and not a technical backwater, the organization must activate, coordinate, deploy, and direct many of its core competencies to create effective solutions. And to sustain success, the organization must move toward a security management process that is strategic, systematic, and repeatable, with efficient use of resources and effective, consistent achievement of goals [Caralli 04].

This is a tall order, but leaders must be up to the challenge. Their behaviors and actions with respect to security influence the rest of the organization. When staff members see the board and executive team giving time and attention to security, they know that security is worth their own time and attention. In this way, a security-conscious culture can grow.

Culture is defined as the predominating, shared attitudes, values, goals, behaviors, and practices that characterize the functioning of a group or organization. The following beliefs, behaviors, capabilities, and actions consistently indicate that an organization is addressing security as a governance and management concern, toward building and reinforcing a security-conscious culture:

- Security is enacted at an enterprise level. Executive-level leaders understand their accountability and responsibility with respect to security for the organization, for their stakeholders, for the communities they serve including the Internet community, and for the protection of critical national infrastructures.
- Security is treated as a business requirement. It is considered a cost of doing business, not a discretionary or negotiable budget-line item. Business units and staff don't get to decide unilaterally how much security they want. Adequate and sustained funding and allocation of security resources are required.
- Security is considered during normal strategic and operational planning cycles. Security has achievable, measurable objectives that directly align with enterprise objectives. Determining how much security is enough equates to how much risk exposure an organization can tolerate.
- All function and business unit leaders within the organization understand how security serves as a business enabler (versus an inhibitor). They view security as one of their responsibilities and understand that their performance with respect to security is measured as part of their overall performance.
- Security is integrated into enterprise functions and processes, including risk management, human resources (hiring and firing), audit/compliance, disaster recovery, business continuity, asset management, change control, applications development, and IT operations. Security is actively considered as part of new-project initiation, ongoing project management, and during all phases of any software-development life cycle.
- All personnel who have access to digital assets and enterprise networks understand their individual responsibilities with respect to protecting and preserving the organization's security. Rewards, recognition, and

consequences with respect to security policy compliance are consistently applied and reinforced.

The Organisation for Economic Co-operation and Development (OECD) also discusses the need to develop a "culture of security" in its *Guidelines for the Security of Information Systems and Networks* (pdf).

References

[Allen 05] 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.

[Caralli 04] Caralli, Richard. "Managing for Enterprise Security" (CMU/SEI-2004-TN-046). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, December 2004. http://www.sei.cmu.edu/library/abstracts/reports/04tn046.cfm.

[DHS 06] Department of Homeland Security Build Security In web site; Governance & Management content area

[Steven 06] Steven, John. "Adopting an Enterprise Software Security Framework." IEEE Security & Privacy, IEEE Computer Society, March/April 2006.

See "Introduction to Security Governance" for a useful table that compares and contrasts a company with effective governance practices and one where these practices are missing. http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1210565,00.html?track=NL-431&ad=559554&asrc=EM_NLT_479998&uid=790142.
