
**SECURITY AND PRIVACY: WHAT BOARD
MEMBERS ARE BEING TOLD TO ASK OF
THEIR MANAGEMENT**

PHOCUS 2003

Joel Lanz, CPA, CISA, CISSP.

www.itriskmgt.com

jlantz@itriskmgt.com

Agenda

- Introduction
 - Key Organizations and What They Are Recommending
 - Regulators
 - American Bar Association
 - National Association of Corporate Directors
 - Institute of Internal Auditors
 - Information Systems and Control Association
 - American Institute of Certified Public Accountants
 - Discussion Forum
 - Questions and Answers
-

Joel's Audit Experience

- Over 22 years of IT risk management experience ranging from one-person “IT shops” to global organizations – specializing in privacy-related industries (e.g., banking and insurance)
 - Principal of a niche technology risk management CPA practice, with prior experience as a Big 5 Technology Risk Partner and an Internal Audit Vice President
 - Adjunct Professor at the School of Professional Accountancy, College of Management, C.W. Post Campus of Long Island University.
 - Member, NYSSCPA Technology Assurance Committee
 - Professional Certifications in addition to CPA
 - Certified Information Systems Security Professional (CISSP)
 - Certified Information Systems Auditor (CISA)
 - Certified Fraud Examiner (CFE)
 - AICPA's Certified Information Technology Professional (CITP)
 - Publications, etc., etc.
-

Regulators and Typical Past Practices

- There was always “some” type of requirement.
 - Board involvement was primarily limited to reviewing and approving security policies.
 - Typical board focus was avoiding “public embarrassment.”
 - They can’t hack us can they?
 - We don’t have an on-line presence so we don’t need to worry.
 - Regulators are overreacting – we’re too small for anyone to want to hack.
 - Regulators were concerned whether Management was adequately addressing security risk with the board
 - As far as board agenda items went, security was not a primary interest of senior executives or board members.
-

501(b) Exam Procedures Puts it in Writing

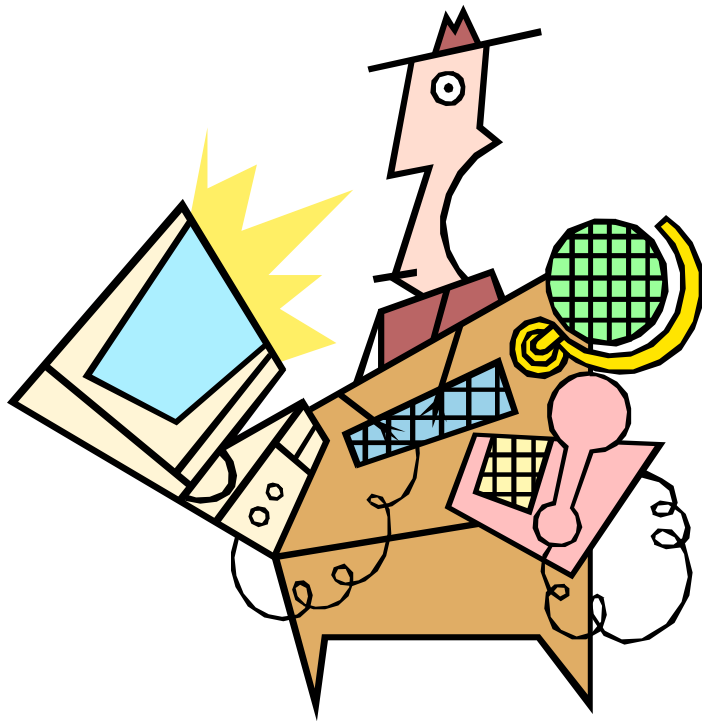
- Has the board or designated committee approved a written corporate information security program that meets the requirements of the information security guidelines?
 - Does the board possess the necessary knowledge, expertise and authority to assign responsibilities for program implementation and review management reports?
 - Determine the usefulness of reports from management to the board. Are key elements adequately described?
 - Overall, does management and the board adequately oversee the information security program?
-

New IT Examination Handbook

Reconfirms Board Responsibilities

- Review board and committee minutes to determine the level of senior management support of and commitment to security.
 - What does this mean (see page 5 of the handbook)?
 - The board of directors is responsible for overseeing the development, implementation and maintenance of the institution's information security program. Oversight requires the board to provide management with guidance and receive reports on the effectiveness of management's response.
 - The board should approve written information security policies and the information security program at least annually.
 - The board should provide management with its expectations and requirements for central oversight and coordination, area of responsibility, risk measurement, monitoring and testing, reporting and acceptable residual risk.
-

Still not convinced?

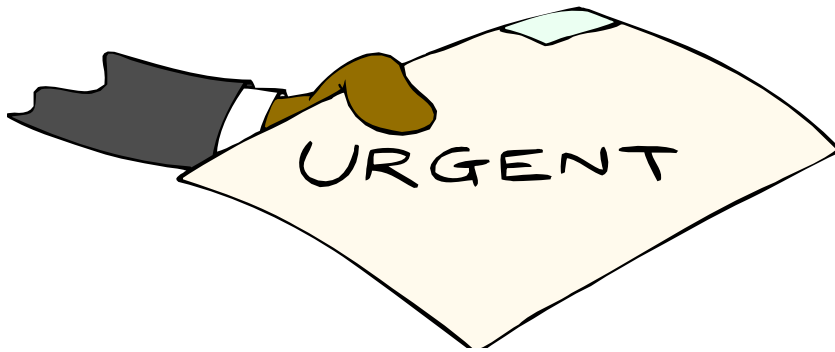


- But Joel, you don't understand (choose one):
 - ❑ Our CEO and how he deals with the board
 - ❑ Our organization
 - ❑ Our board and their lack of technology or security know-how
 - ❑ Our uniqueness
 - ❑ Our other priorities
-

American Bar Association – Information Security Committee

- “The Information Security Handbook Work Group, one of the two new work groups of the ISC, will continue progress on the Information Security Handbook, a document that addresses information security basics, **including a due care standard for negligent liability**, for private companies and organizations”.
-

Now do I have your attention?



- How do we start?
 - Where do we go to get information?
 - What are others doing?
 - What are the expectations?
 - How will we prepare our board?
-

Understand Why Information Security Needs to be Governed

- Risks and threats are real and can significantly impact the organization
- Effective information security requires co-ordinated and integrated action from the top
- Investments can be substantial and misunderstood
- Culture and politics of the organization may unduly influence
- Rules and priorities need to be established and enforced
- Trust needs to be demonstrated to business partners and customers
- Security incidents are likely to be exposed to the public
- Considerable reputational damages

Source: Information Security Governance, IT Governance Institute

Unprecedented Guidance

- “Information Security Oversight: Essential Board Practices.” National Association of Corporate Directors.
 - “Information Security Governance: What Directors Need to Know.” The Institute of Internal Auditors (Critical Infrastructure Assurance Project).
 - “Information Security Governance: Guidance for Boards of Directors and Executive Management.” IT Governance Institute (affiliated with Information Systems Audit and Control Association).
 - “Board Briefing on IT Governance.” IT Governance Institute (affiliated with Information Systems Audit and Control Association).
-

Guidance is in Collaboration with

- Big Accounting Firms
 - Key Government Agencies
 - U.S. Department of Commerce
 - U.S. Professional Organizations
 - International CPA Organizations
 - Key Vendors and Consultants
 - Gartner
 - SANS Institute
-

NACD's Four Essential Board Practices

- Place Information Security on the Board's Agenda
 - Identify Information Security Leaders, Hold Them Accountable, and Ensure Support for Them
 - Ensure the Effectiveness of the Corporation's Information Security Policy Through Review and Approval
 - Assign Information Security to a Key Committee and Ensure Adequate Support for That Committee
-

Place Information Security on the Board's Agenda

- Make information security a regular agenda item at board meetings (annual at a minimum)
 - Ask management to report regularly on the state of information security
 - Include information security in the board's risk management discussions
 - Learn more about the company's information security risk management policy and procedures
-

Identify Information Security Leaders, Hold Them Accountable, and Ensure Support for Them

- Find out who is in charge of information security and to whom the person reports.
 - Identify the role and resources of the internal auditor with respect to information security.
 - Ensure education for the individuals involved and for all employees
 - Consider asking management to review and test policies using independent (including internal audit) testers
-

Ensure the Effectiveness of the Corporation's Information Security Policy Through Review & Approval

- Review the corporation's existing information policy, or, if there is no policy, encourage management to develop one
 - Review the company's internal controls with regard to information security (especially with the enactment of Sarbanes
 - Working with management, identify the greatest risks to the company's information security resources
 - Ensure that appropriate vendor management reviews are in place for company contractors
-

Assign Information Security to a Key Committee and Ensure Adequate Support for That Committee

- Consider delegating information security to a qualified board-level committee that can devote the time needed for this task, and write information security oversight into the committee's charter
 - Consider information security oversight a potential area for audit coverage
 - Involve the audit committee in reviewing policies and procedures
 - Make full use of the internal audit function in creating and following information security oversight policies
-

The 10 Questions Boards Should Ask

Source: *Information Security Governance: What Directors Need to Know*

- What management system have we established to assure effective **assignment of accountability** for the security of our information and supporting technology resources?
 - *Management is responsible and the board accountable*
 - What has management done to assure that all **parties know, understand, and accept** the importance of adhering to sound information security?
 - *Security awareness starts with the board and permeates the organization*
 - What has management done to assure that we are **using our information assets** and administering information security in an ethical manner?
 - *Codes of conduct are followed in the use of computers as in other activities*
 - What has management done to assure that the perspectives and **considerations of all interested and affected parties** are considered and balanced in developing our information security policy?
 - *Security achieved through combined efforts of all and mindful of all participants*
 - What **cost/benefit, risk, and due care analyses** have been applied to the selection of our information security controls?
 - *Security decisions made as others – management recommends and the board concurs*
-

The 10 Questions Boards Should Ask

(cont.)

- How has management coordinated and integrated information security with our **overall policies and procedures** to create and maintain effective security throughout our information systems?
 - *Security must be integrated into all relevant organizational policies*
- What capabilities do we have to assure that **failures involving information technology** or its management will not endanger the organization, its supported business units, its neighbors, or their information assets, and will not impair their ability to operate? (Consider requirements for timeliness, availability, and reliability.)
 - *As other risks, mitigate based on cost-effectiveness (and risk assessment)*
- What capabilities do we have to assure that risks associated with information and supporting technology resources are **effectively assessed on an appropriate periodic basis**, or as otherwise required, and managed accordingly?
 - *Require periodic reporting by management and independent assessments by audit*
- How does management assure that our information **security measures are fair and legal**?
 - *Coordinate with the audit committee who are typically responsible for these issues*
- How effectively does management **share appropriate information with our peer organizations** and appropriate governmental entities?
 - *Get a plan together based on current practices and reviewed by relevant functions (e.g., legal, marketing, customer relationship, etc.)*

Thought-Provoking Questions for Board Members (Can Management Provide Answers)

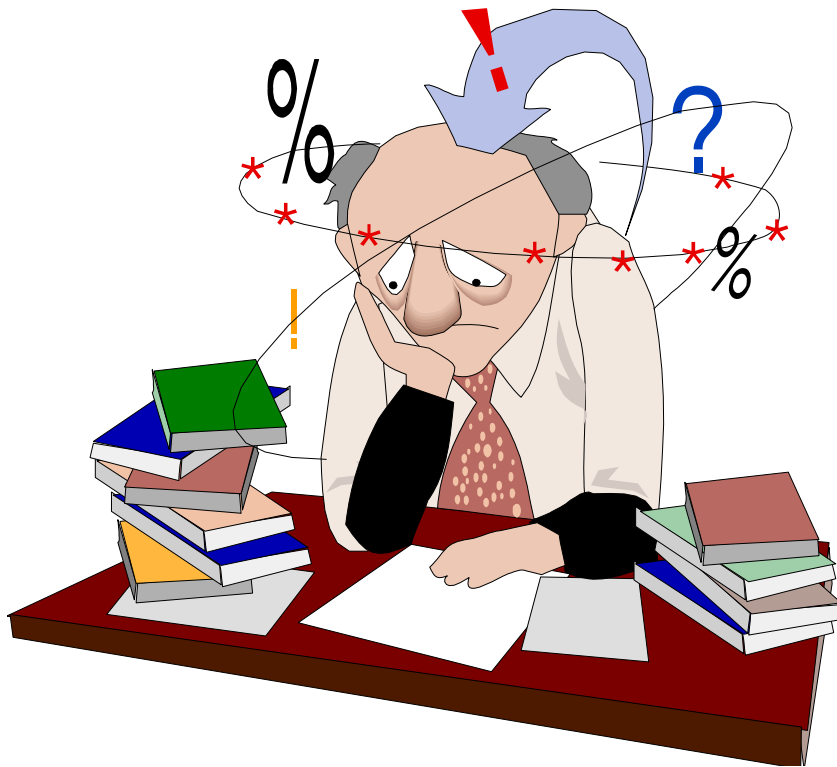
- When was the last time top management got involved in security related decisions?
- Does management know who is responsible for security?
- Would people recognize a security incident if they saw one?
- Does anyone have an inventory of all our information technology assets?
- Has management identified all information (customer, data, strategic plans) that would cause embarrassment or competitive disadvantage if it were leaked?
- Did the company suffer from the latest virus attack?
- Is the enterprise network being probed? Have there been intrusions? How often and with what impact?
- Does anyone know how many authorized users we have and what they are doing with these system privileges?
- Is security considered an afterthought?
- What would be the consequences of a serious security incident in terms of lost revenues, lost customers and investor confidence?

Source: Information Security Governance: Guidance for Boards of Directors and Executive Management

Your Next Steps

- “Street-smart” Technology Risk Assessment
 - Based on recognized standards
 - Tied-in to things that the board should be concerned about
 - Identify target security maturity level
 - Obtain board “buy-in”
 - Manage to the level
 - Identify relevant issues discussed today
 - Leverage references to develop appropriate board package
 - Invest in security awareness training for the board
-

QUESTIONS OR FURTHER INFO



Joel Lanz, Principal
Joel Lanz, CPA, P.C.
P.O. Box 597
Jericho, NY 117530597
PH: 516-933-3662
FX: 516-933-2885
jlanz@itriskmgt.com
www.joellanzcpa.com
www.itriskmgt.com
