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

The Legal Side of Global Security

Key Message: Business leaders, including legal counsel, need to understand how to tackle complex security issues for a global enterprise.

Executive Summary

In this podcast, Jody Westby, CEO of Global Cyber Risk and Chair of the American Bar Association's Privacy and Computer Crime Committee, talks about a range of security-related issues when conducting business in a global marketplace. These include protecting data as it travels across borders, outsourcing operations, understanding jurisdiction differences and protecting client and work-product privilege, and tackling the new roles that legal counsel and business leaders need to fill.

PART 1: THE COMPLEXITY OF INFORMATION PROTECTION

PII (Personally Identifiable Information) is protected by most privacy legislation and can include:

- name, address, and telephone number
- employment and purchasing history
- sexual and religious preferences
- cable TV records, insurance records, school records, arrest records, and driving records - which many people do not realize is protected by, at least, U.S. law

Protecting data that flows from country to country is a complex issue in many situations:

- when moving from a country with specific protections to a country with different protections (such as from the U.S. to one of the 25 member countries of the European Union), or when moving to a country with no protections
- when dealing with the inconsistency of laws between countries when something "illegal" happens, including procedures for international cooperation
- when considering the wide disparity of skill levels of law enforcement
- taking into account the differences between developed and developing countries

The Council of Europe Convention on Cyber Crime has made progress toward addressing some of these issues.

PART 2: CHALLENGES FOR GLOBAL OPERATIONS; ROLES AND RESPONSIBILITIES

Issues that arise when dealing with global, outsourced operations and global supply chains include:

- the differences in governance, compliance, and legal requirements among various countries and companies
- how to determine what your supplier or partner is doing to meet your compliance and security requirements, through contracts and adequate monitoring and reporting
- a lack of understanding that outsourcing a function does not mean outsourcing your governance and compliance requirements for that function

When dealing with cyber crime, global organizations need to understand how to adapt and tailor their in-country requirements for local jurisdictions, customs, and cultures.

So, who is in the best position to tackle these issues?

- The Board Risk Committee, CEO, and senior management
- A cross-organizational (X) team that includes general counsel, human resources, chief security (CSO) and chief information security (CISO) officers, chief risk officer, chief privacy officer, procurement, communications, and public relations
- Operational personnel including asset owners, responsible for information, applications, and networks

The cross-organizational team is a critical key to success. Its members are responsible for ensuring security requirements are addressed in day-to-day operations throughout the organization.

The CSO or CISO has primary responsibility for developing and executing the enterprise security program (ESP).

PART 3: THE ROLE OF LEGAL COUNSEL IN A GLOBAL ENTERPRISE

Legal counsel needs to understand:

- how to convey contractual provisions that require privacy or security measures to operational business and technical teams
- their leadership role in the development of an ESP
- the categorization of digital assets, as this is often key to meeting compliance requirements
- how and when to use privilege, both attorney-client and attorney-work-product, and when work should be performed by in-house or outside counsel to protect privilege

Issues such as privilege are very important when dealing with forensic investigations of a security incident and the potential for class-action lawsuits.

Legal counsel needs to address the following potential pitfalls:

- Developing new skills and competencies to deal with enterprise and information security requirements
- How to manage legal liabilities without impacting business operations
- How to balance risk and reward

PART 4: WHAT LEADERS CAN DO

So, what can leaders do to address these issues?

- Create an effective cross-organizational team. Encourage open and candid exchange of diverse ideas and solutions, and achieve buy-in.
- Define and assign clear roles and responsibilities, including appropriate segregation of duties.
- Make sure critical assets and processes are identified and properly categorized.
- Develop an enterprise risk management plan that addresses security. Ensure that it integrates security with business continuity, crisis communications, and incident response.
- Develop key messages and points of contact in the event of an incident.
- Provide adequate resources, understanding that security is a continuous process.
- Provide adequate and recurring training at all levels and for all roles.

CSOs and CISOs need to be able to convey their value proposition in terms that business leaders, executives, and board members will understand.

Resources for Staying Up to Date

CERT's Governing for Enterprise Security portal

The Department of Homeland Security's US-CERT

American Bar Association Privacy and Computer Crime Committee

The Information Systems Audit and Control Association

The IT Governance Institute

The Institute of Internal Auditors