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

Protecting Information Privacy: How To and Lessons Learned

Key Message: Aligning with business objectives, integrating with enterprise risks, and collaborating with stakeholders are key to ensuring information privacy.

Executive Summary

Privacy is demanding an increasing share of business leaders' attention due to the growing number of laws and regulations and the growing number of unauthorized disclosures of sensitive, personal information. While there are some common issues and solutions between information privacy and information security, privacy is more concerned with content and use, and thus has some unique challenges.

In this podcast, Kim Hargraves, Director of Trustworthy Computing Strategy for Microsoft, discusses the growing importance of information privacy, how to use privacy risk assessment to jump start your privacy program, and lessons learned.

PART 1: WHY SHOULD PRIVACY BE ON A BUSINESS LEADER'S RADAR SCREEN?

Growing Demand for Information Privacy

This is due to:

- increasing digitization of personal data
- globalization of economies and supply chains
- increasing information flow within and across borders, and between organization
- a growing concern for governments, businesses, and consumers
- regulatory compliance
- highly publicized data breaches affecting more than 100 million users

C-level executives are increasingly paying attention, as poor privacy practices can lead to erosion of trust, which can ultimately impact revenue.

It is often difficult to reconcile different privacy laws and regulations among the U.S., Canada, Europe, and Asia-Pacific.

For Microsoft (and other large global organizations), it is challenging to figure out where the bar is from a legal perspective. But even working this out can be insufficient due to customer expectations of privacy, which differs from country to country.

How Privacy Differs from Security

Information security and information privacy are often viewed as the same problem with the same solutions.

Security vulnerabilities can lead to a breach or inappropriate disclosure of personal information. However privacy is much broader than security. You need to consider:

- How is personal data going to be used? What restrictions has the individual placed on use of their data?
- What business processes access this data?
- How will marketing and human resources business process issues, for example, be addressed?

When you think about security, you often think about controls. With privacy, you also need to address:

- What implications arise from data content and intention of data use?
- Who is gathering the data?
- Is data use consistent with the organization's privacy principles and statements?
- Does data use align with legal and regulatory requirements?

There is much more involvement of the human element in privacy.

PART 2: THE BENEFITS OF A PRIVACY RISK ASSESSMENT

How Can a Privacy Risk Assessment Help Select What Risks To Mitigate?

A risk assessment program needs to be part of a larger risk management strategy.

A risk assessment allows you to identify, capture, and prioritize risks.

A risk assessment is a collaborative process involving the right stakeholders – those who have control over purse strings and over resource allocation.

The risk assessment and the results must align with business objectives.

Once you have business ownership of the process and the results, real change can occur through implementing effective risk mitigation strategies.

Generating Enthusiasm with Business Leaders and Information Owners

Recognize that business units in most organization are diverse. In Microsoft, there are significant differences between shared services organizations (for example, Human Resources and Finance), product development organizations (software in a box), online services, and consumer products (Xbox).

Spend time understanding each business unit, what drives it, and its cultural differences – and be willing to adjust the risk assessment program based on what you learn.

Work in a collaborative way to tailor action plans.

Frame privacy issues and concerns in business terms and make sure they are aligned with business objectives.

Integrating Privacy Risk Assessment at the Enterprise Level

There are many different types of risk assessment – financial, capital, operational, and information security, to name a few.

Integrating privacy risk assessments into the mix can be accomplished by adopting an enterprise risk management (ERM) strategy.

This allows business leaders to place the right risk assessment activities with the right level and for the right areas of the company.

The COSO ERM Integrated Framework provides useful guidance. It includes four pillars of concentration:

- financial reporting risks
- operational risks
- legal and regulatory risks

- strategic risks

Microsoft has an owner for each risk pillar.

Privacy risks can be placed in each of these four areas, which allow them to be considered in the mix with other enterprise risks. This appears to be much more effective than dealing with domain-specific risks (security, privacy, employment law, etc.).

An ERM approach allows risks to be addressed and prioritized much more holistically. That said, this is a challenging approach that takes time to define and implement.

PART 3: LESSONS LEARNED

Training and Collaboration Are Key

- Be flexible, given that business units operate differently.
- Start off by building a basis of understanding of the privacy subject.
- Training is critical. Start with Privacy 101 that is relevant for all employees.
- Develop and use role-based training for specific segments of the organization (product development, marketing, database administration, to name a few).
- Use a risk-based approach to define the privacy strategy and ensure it aligns with business objectives. This alignment is key.
- Do not make privacy a legal and regulatory compliance exercise.
- Do not implement privacy in a silo. Partner and collaborate with key stakeholder organizations, such as internal audit.

Microsoft conducted a recent study with the Ponemon Institute, investigating the different roles between marketing, privacy, and security organizations across the company. The intent was to understand the level of collaboration and its value, if any.

The study revealed a strong correlation between level of collaboration and incidence of data breaches.

Where collaboration is strong, these organizations are much less likely to suffer a data breach than where collaboration is weak.

Critical for program success is taking the time up front to get shareholders and stakeholders on board, create collaboration structures, and establish relationship networks.

Resources

Microsoft's Trustworthy Computing Program