Business Privacy in the Cloud: Imperative for Data Protection

Q&A with Heidi Shey of Forrester Research

Heidi Shey, Senior Analyst Security and Risk,
FORRESTER®

Q: What are the most critical challenges organizations face today in terms of ensuring business privacy and data security? Who should be most concerned?

The biggest thing I see is a tendency to start from a position of focusing on tactical efforts like implementing a particular technology or issuing a specific policy. In these cases, there's a lack of higher level strategy for business privacy and data security. Decisions about data controls are primarily reactive and compliance-driven. Often there isn't a consistent understanding of what constitutes toxic data, or data that would be harmful to the organization if compromised, exposed, or lost. Toxic data includes sensitive corporate data like intellectual property as well as regulated data like personal information, healthcare information, or cardholder data that would typically fall under compliance requirements. Organizations must realize that privacy and data security aren't simply the concern of IT and security leaders. The board of directors, CEO, and line of business executives should all be concerned because business privacy and data security are matters of competitive differentiation and reputational risk today.

Q: Investments in business privacy and data security could potentially offer both ROI and risk mitigation benefits. How should IT leaders develop the business case for these investments? How do you quantify the benefits?

You cannot ignore rising regulatory penalties and fines; EU GDPR has penalties of up to 4% of annual revenue or €20 Million (whichever is greater), a settlement with the US FTC could involve 20 years' worth of audits. HIPAA and PCI also have monetary penalties for violations. Yet solely focusing on costs of a breach or privacy violations presents a narrow perspective for developing a business case. Look to build a business case that highlights the value of data to the organization's mission, as well as to customer and business partner trust. How does data contribute to revenue and growth in dollar terms? Recognize that it's not just about protecting the data you currently have and use, but maintaining a good reputation and trust in your organization to enable customers and partners to continue sharing their data and doing business with you. This is important for building trust with your investors and board members too. Also recognize the importance of protecting your employee data, and what that means for your organization's future hiring efforts and ability to attract talent.

Q: Please describe the underlying trends that are driving the need to business privacy technologies?

Evolving privacy laws around the world are helping to force enterprise discussions around data storage, data transfer, data collection purpose and consent. Companies must implement reasonable measures and technology controls for data protection that enable employees to securely access, use, and share information necessary to do their jobs. This is increasingly critical as more and more organizations move email and file shares to the cloud. Regulatory and technology trends aside, social factors are another major trend. The notion that privacy is dead or that consumers don't care about privacy is outdated. Our research has defined key attributes and behaviors that determine a consumer's privacy segmentation and their willingness to share data.[1] This makes having a strategy for data protection and enabling the right tools to support that strategy a critical priority. Data protection is a corporate social responsibility and business edge in this age of the customer and digital business. Companies that realize this understand that missteps with data use and handling – whether it's lax measures to secure the data or unethical use of data – are not attributes they want associated with their organization.

[1] This report uses Forrester's Consumer Technographics research to define four consumer segments as well as their attitudes and behaviors relating to marketers' collection and use of personal data. https://www.forrester.com/report/Introducing+Forresters+Consumer+Privacy+Segmentation/-/E-RES119986

Q: As businesses move to cloud-based systems for email and other types of data sharing, what are the business privacy risks and opportunities they should be reviewing?

Recognize that data is a living thing that no longer resides in a static location; you need data-centric security controls to ensure that protection travels with the data no matter where it goes -- cloud, on-premise, or on mobile devices. On the business side, identify your organization's toxic data, what is shared and stored in cloud versus on premise, how data needs to flow and how it is used. This will provide the foundation for assessing the privacy risks. To assess opportunities, determine how this data is used, what workflows and business processes it supports. This can help to determine where you might streamline certain processes or identify new use cases for the business. On the cloud provider side, make sure you understand their security capabilities and controls. Where is the data stored? Who holds the encryption keys? What unencrypted content do they have access to? What assurances can they provide? Have you and your provider outlined responsibilities in the event of a breach? Does your organization have a plan for backup and resiliency? What third-party providers integrate with your cloud provider to offer additional layers of data security or business privacy?

Q: What are the most important factors the businesses should consider when evaluating business privacy technologies and initiatives?

Recognize that it's not a single technology, but combination of tools, processes, and policies that you will need to address data security and business privacy. A risk and maturity assessment will help you prioritize investments based on the areas of greatest risk and impact to your highest value data. With technologies, take care to evaluate enterprise fit and usability as key factors. How does this technology work with other applications or tools within your environment? Also understand how data is used and why, and what your employees need to do with data in order to do their jobs as well as how your employees get their job done. What are the needs of an employee working primarily in the office versus your road warriors or remote workers? A technology that is easy to use that employees will want to use is important; otherwise you set yourself up for a scenario where employees actively look for workarounds because you haven't met their needs.