JMBM
Jeffer Mangels Butler & Mitchell LLP
jmbm.com

Meet the Money® Online

Best Practices and Imperatives

Robert E. Braun
Partner & Co-chair
Cybersecurity and Privacy Law Group

June 25, 2020

Robert E. Braun

Robert E. Braun is the co-chair of the Cybersecurity and Privacy Law Group at Jeffer Mangels Butler & Mitchell LLP and a senior member of the JMBM Global Hospitality Group. Bob helps clients to develop and implement privacy and information security policies, negotiate technology and management agreements, and comply with legal and regulatory requirements. He helps clients to develop and implement data breach response plans and respond quickly to clients' needs when a data breach occurs.

Contact Bob at RBraun@jmbm.com or 310.785.5331.

Disclaimer

Nothing contained in this presentation is intended to provide legal advice to any person or entity.

Why is Information Security So Hard?

What Stands in the Way of Effective Information Security?

- There is no such thing as perfect information security
- Misunderstandings about what is reasonable information security
- Existing frameworks do not, by themselves, deliver reasonable information security
- Effective information security requires people and process, not just technology
- Dynamic changes in the workplace which shift the risk landscape

Imperatives for Privacy and Information Security

What Drives Privacy and Information Security?

- Statutes, Regulations and Orders
  - CCPA
  - FTC and State Regulation
  - Judicial Rulings
- Industry guidelines and frameworks
- Reputation
- Business damage – DOS, ransomware and wiperware

The Goal: Actual Cybersecurity

- Actual security vs. compliance
  - Compliance is checking boxes on a list that doesn't necessarily reflect your operations
  - Actual security is achieving security for operations – and it usually leads to compliance
- Actual security requires a deep dive into how a firm collects (or obtains), what they use it for, who has access to it, and how it is held.
- Actual data security must be validated and documented

Privacy and Security Challenges in Hospitality

Allocation of Risk

- Who's responsible?
  - Brands – from reservations and loyalty programs?
  - Managers – from on-site data collection?
  - Owners – because owners somehow end up paying for all of it – whether it be increased costs or penalties for non-compliance
- Who "owns" and who uses a guest's personal information?

Achieving Effective Information Security

Key Steps to Cybersecurity

- Contextual to the organization
- Based on data flows and network architecture
- Inclusion of all data points, including external sources and users
- Written policies that are disseminated to all personnel
- Effective data/information governance
- Regular revision and testing

Third Parties and Privacy

Vendors and Other Third Parties

- All enterprises require third parties (cloud services, data processors, etc.)
  - Parties to whom do you disclose data
  - Parties from whom you receive data
  - Their vendors and third parties
- Third parties are a key element in information security
- Key vendors need to be verified; representations are not adequate

Takeaways

Key Takeaways

- Information security is bespoken – there is no “one size fits all” approach
- Reasonable security requires documentation
- Information security is fluid – it needs to be reviewed regularly and anytime there are changes to the system

Questions

JMBM Jeffer Mangels Butler & Mitchell LLP

jmbm.com

THE END

For additional information, point your browser to https://www.jmbm.com/cybersecurity-and-privacy-group.html

You can subscribe to our blog, the Cybersecurity Lawyer at https://cybersecurity.jmbm.com/

And you can contact Bob at RBraun@jmbm.com or 310.785.5331