Data in Hospitality: Are You Keeping Up?

By Patrick R. Grady, Manager, Thomas J. DeMayo, Principal, and Ronald R. Martinez, Senior Manager

In today's fast paced world, organizations in the hospitality industry face an ever-growing need to adapt quickly to technology. Without due diligence and protective measures in place, businesses are increasingly vulnerable to risks posed by the constantly changing information technology landscape. Avoiding external threats and internal risks requires staying up to date with the evolving hardware, software and data used throughout the industry.

As new technologies are implemented into hospitality operations, the amount of data collected increases exponentially. Modernization is dramatically expanding the amount of sensitive data collected and stored by hospitality operations. As a result, data security is paramount for businesses exposed to internal and external threats.

Sensitive data originates from the daily operational activities inherent in every hospitality organization including:

- Guest relations and loyalty programs
- Keycard entry to guest rooms and other restricted areas
- Recording of transactions and collection of guest data through point of sale (POS) and property management (PMS) systems
- Back office accounting and finance functions
- Payroll, credit card processing and other outsourced functions

It is crucial to understand the source of data and how it is stored. Data from these activities falls into two categories: private customer data and business financial data. A closer look at each is revealing:

Private Customer Data

Both personal and financial information collected from customers have compliance requirements that must be considered to ensure data security. Two major areas of compliance are the EU's General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standards (PCI DSS).

- **GDPR** – When operating a hotel marketed to international travelers from the European Union, compliance with the GDPR is a requirement as governance reaches farther than the EU's borders. The GDPR is designed to ensure the privacy of every individual's personal data and governs how a business uses the data collected from customers. GDPR requires that businesses clearly disclose any data collection and inform customers of the purpose of the data collection, how long the data is retained and whether the data will be shared with any third parties outside the European Economic Area.

- **PCI DSS** - Credit and debit cards are the most common way customers pay for goods and services. PCI DSS is not required by federal law in the USA, but these standards are mandated by major credit card brands and many states have laws referencing the standards. PCI DSS increases and strengthens controls surrounding credit cards and reduces credit card fraud.

Technical and operational system components included or connected to cardholder data are covered by PCI DSS. When choosing a PMS or POS system, the integration of PCI DSS technology must be considered.

Any breach of customer data damages a business's public image and trust. The compliance landscape extending beyond GDPR and PCI DSS is evolving and complex. A cybersecurity and privacy risk assessment by a third party can help ensure that the business's customer data is protected from potential threats, that compliance obligations are fully understood and managed and that the business is readily positioned to embrace and adopt evolving technologies.

Business Financial Data

Equally as important as customer data is the business's financial data. A breach could result in financial losses to the business. Company bank accounts, corporate credit cards and financial records are all at risk. Steps to protect the business include:

- Encryption
  - Sensitive data encryption
  - Password protected accounting spreadsheets
- Restriction
  - Limited access to bank accounts and corporate cards
  - Restricted access to accounting, property management and point of sale systems
- Verification
  - Routine trainings for employees regarding information systems security
  - IT audits, cyber security reviews and penetration tests

Even when outsourced to an external party, certain business functions – of which payroll and credit card processing are the most common – remain the business's responsibility. It is the business that must oversee these services and ensure that data is properly handled. Obtaining a System and Organization Control Report Type 2 (SOC 1 Type 2 Report) can aid in the evaluation of the vendors, providing assurance that the service organization has the necessary controls in place to protect the business's data and financial assets.

A SOC 1 Type 2 Report details the controls and activities at an outsourced vendor and attests to the design and suitability of the controls, as well as whether they are operating effectively. Reviewing the report for relevance to the business, its data and exceptions in operating effectiveness can help identify weaknesses and security gaps. Obtaining a prospective vendor's SOC 1 Type 2 Report is a significant step towards identifying potential problems and gaining valuable insights about future data risks. Additionally, it is important that the business ensures that identified user entity controls within the report are addressed as part of its internal controls.

Further Steps

When a business's information systems and data grow in complexity it may become necessary to enlist a third party to aid in the planning, design and implementation of new technologies. Consultants and independent auditors can provide valuable services, such as:

- IT audit, which is a detailed examination and evaluation of an organization's information technology infrastructure, policies and operations.

- Cybersecurity review, which provides an in-depth independent assessment of a business's ability to protect its data and financial assets from cyber threats.
- Assistance with design and implementation of IT systems.
- Virtual Chief Information Security Officer services to manage and guide a business's cybersecurity and privacy programs.

These services provide feedback and evaluations about a business's IT environment that can confirm that the preventive and risk mitigation measures are adequate or recommend steps to be taken to address vulnerabilities.

Contact Us

PKF O'Connor Davies offers an array of services and expertise to the hospitality industry. If you have any questions on these or other topics addressed here, relating to the hospitality industry, we invite you to contact our hospitality industry specialists.

Patrick R. Grady
Manager
pgrady@pkfod.com

Thomas J. DeMayo
Principal
tdemayo@pkfod.com

Ronald R. Martinez
Senior Manager
rmartinez@pkfod.com

About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, twelve offices in New York, New Jersey, Connecticut, Maryland and Rhode Island, and more than 800 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is ranked 27th on *Accounting Today*'s 2020 "Top 100 Firms" list. It is also ranked among the top 20 best accounting employers to work for in North America by *Vault*.

PKF O'Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.