WHAT ARE THE CONTROLLER'S AND CFO'S ROLES IN DATA SECURITY?

Reduce Risk by Taking Action

By Julie Eisenhauer, CPA, and Peter Henley, CPA, CITP

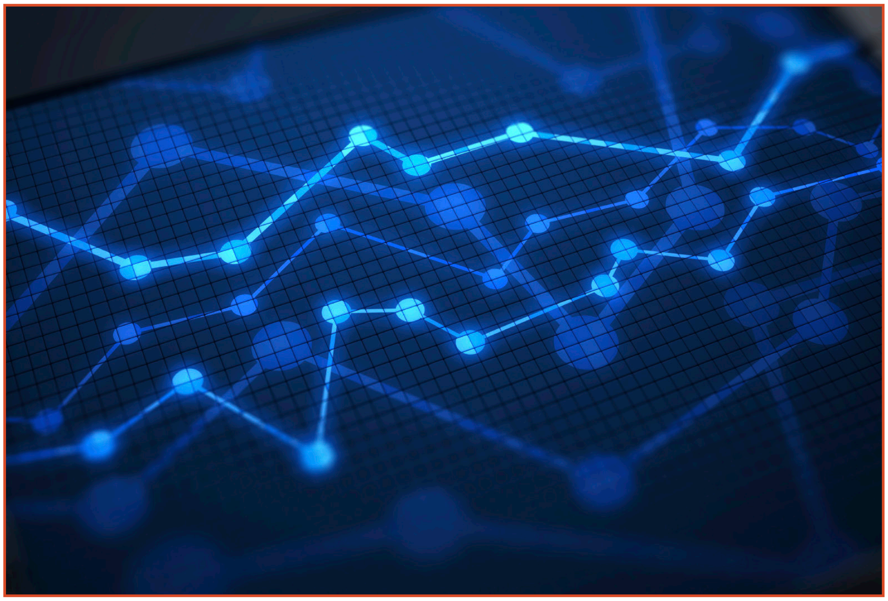
Data breaches strike all industries, but for the hospitality industry the stakes are extremely high, and the financial impact to a company can be significant. As the ones who watch over the company's financial performance, controllers and CFOs must manage all components that impact the bottom line and that includes corporate data. Not securing data results in three serious threats to the company.

- Strategic losses
- Regulatory penalties
- Brand reputation damage

We've all read the news about data breaches. The financial consequences and reputation damage have been widely reported. Each new incident makes it clear that businesses both large and small need to address security and assurance.

Key Statistics

- An estimated 78 percent of all companies and organizations in the United States suffered some sort of data loss or theft within the last two years.
- 44 percent of small businesses state that they have been a victim of cybercrime of some kind at least once.



- More than half of U.S. small businesses have experienced at least one data breach.
- 75 percent of respondents in a recent survey say they've had or expect to have a data breach that results in negative publicity.

(Data derived from the Verizon 2014 Data Breach Investigation Report and the Ponemon Institute 2013 Report.)

Why Controllers and CFOs are Getting Involved

In an informal survey we conducted of controllers and CFOs working for companies in the hospitality and retail industries, 93 percent stated that they frequently encounter technology-related questions or concerns in their role at the company. This survey also revealed that 36 percent were very confident in their understanding of the risks associated with information technology, while 64 percent were somewhat confident.

Julie Eisenhauer is an audit and assurance shareholder at Clark Nuber PS (jeisenhauer@clarknuber.com / @EisenhauerJulie). Peter Henley is senior director of IT at Clark Nuber PS (phenley@clarknuber.com / @peterhenley).

In a recent survey of U.S. accounting professionals performed by the American Institute of Certified Public Accountants, securing the IT environment was listed as a top technology priority. This was the eighth time over the last 10 surveys that this priority was on the top of the list.

Following the significant data breaches that have occurred over the last few years, is managing IT security the "new normal" for controllers and CFOs? The recent survey results suggest that it is. Controllers and CFOs must take a more comprehensive approach to the financial health of the company by addressing IT in enterprise risk assessments on an ongoing basis.

The controller and CFO should understand what kind of data that hackers are going after, where an attack could come from, as well as what mitigations are in place to prevent the attacks. The CFO and/or controller need to ask the right questions of IT around data security. Focus should be on risks that have a high likelihood and a substantial impact on the business.

> " Following the significant data breaches that have occurred over the last few years, is managing IT security the "new normal" for controllers and CFOs? The recent survey results suggest that it is. Controllers and CFOs must take a more comprehensive approach to the financial health of the company by addressing IT in enterprise risk assessments on an ongoing basis."

5 Practical Steps

Security industry experts state that data breaches are unavoidable. It's not a question of "if" companies will become victims of a data breach, but "when." However, there are five practical steps a business can take to help protect against data breaches and mitigate the potential harm in the event of a breach.

1. Perform an Inventory

It is critical to inventory the locations that store personally identifiable information (PII). PII is defined as information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Personal information includes such things as first and last names, social security number, biometric records, date and place of birth, mother's maiden name, address, e-mail address, driver's license number, or financial account information. Determine which PII information your business requires, what data are collected, how these data are secured and who has access to the data and under what circumstances. Once you have identified the location of your data, move it to more appropriate locations as needed.

2. Encrypt Computers

It is a best practice to encrypt all laptops and publicly accessible desktop computers. Encryption encodes messages or information on a computer in a way that only authorized individuals can read. It doesn't prevent intrusion, but it does make the data unreadable and unusable by an intruder. Encryption software is affordable and highly effective in protecting data. Consider using a data encryption method that is FIPS certified (Federal Information Processing Standard), which means it has been certified for compliance with federal government security protocols. Frequently monitor your systems to ensure that the encryption is still active.

3. Implement an Intrusion Detection System

An intrusion detection system includes a device or software application that monitors network or system activities for malicious activity. Detecting an intrusion early allows for a quicker response, reducing the cost per data record stolen. In order to determine what is considered malicious or "unusual" activity, the business should first define what is considered "normal" activity, based on the nature of their business.

4. Develop a Detailed Plan For Quicker Response

Every business should plan for the unexpected and that includes the loss or theft of data from your business. Businesses that implement a data breach response plan have the tools to act quickly, reducing the harm caused by a data security breach. The plan should document the names of the response team members, including outside vendors such as the attorney, forensic accounting and/or IT security firm and insurance broker. The plan should also document the steps to access the scope of the breach and secure the premises, identify compromised data and eradicate hacker tools, and establish guidelines for notification.

5. Train your staff

Businesses train their staff for daily, on-the-job duties. If you haven't already done so, expand staff training to include the appropriate use of your computer systems, assessing and transferring data, safe web browsing rules, and how to identify threats such as phishing. Encourage your employees to use passwords that are random, complex, changed regularly and that are closely guarded and not written down. Ensure all staff are trained on recognizing suspicious activity and that they are familiar with the company's data security plan.

A data breach can have great consequences that include not only the direct costs of attorneys and forensic experts, but also the indirect costs resulting in the loss of customers and damage to your brand. Take action now to secure your important data and mitigate the potential harm in the event of a breach. ■