Achieving
Higher
Expectations

COSO Framework for Service Organizations and SOC Reporting (Part 3 of 3)

In part 1 of this series, we discussed the recent changes to the COSO framework and the overall impact that the updated framework has on service organizations that receive Service Organization Controls (SOC) reports. Three of the differences that were identified between the 1992 and 2013 Framework that impact service organizations are as follows:

1. Emphasis on understanding and evaluating controls of outsourced service providers (OSPs).
2. Emphasis on risk assessment and fraud risk assessment.
3. Emphasis on IT controls.

In the first 2 posts, we discussed items #1 and 2 above. The objective of this post is to discuss the increased emphasis on IT controls.

One of the most significant changes that businesses have experienced between the release of COSO's 1992 and 2013 frameworks is the automation of processes and controls and the increased reliance on IT. While COSO's 1992 framework included very general and high level information about IT controls, the 2013 framework includes much more specific guidance.

The 2013 framework classifies the key IT General Controls (ITGCs) as follows:

- Technology infrastructure
- Security management processes
- Technology acquisition, development and maintenance processes

For purposes of this blog post, I would like to comment on the relevance of security management to service organizations who receive a SOC 1 or SOC 2 report. One of the trends I have noticed lately on SOC engagements (for both large and small organizations) is that most companies have established strong controls over access to their data, operating system, network, application and physical layers. They make significant investments in controlling their perimeter with sophisticated devices and technology. They are doing all of the right things with regards to technical controls, but don't pay enough attention to basic security awareness training for their employees. This training can be invaluable for protecting companies from hackers and limiting the damage companies could suffer if cybercriminals attack.

The 2015 Data Breach Investigations Report released recently by Verizon Enterprise Solutions includes some very interesting information that should motivate companies to focus more heavily on security awareness training. For example, most hacker attacks in 2014 started when someone responded to a phishing email that allowed hackers access into the system. Verizon found that 23% of all recipients of phishing scams still open such emails and 11% click on the attachments!

During SOC engagements, many of our clients ask me what an effective security awareness training program looks like. My response will vary depending on the nature of the company's business and the type of data that they store or process. In most cases, however, I recommend that, at a minimum, each and every employee attend a 1-2 hour annual security awareness training course that explains the latest vulnerabilities that are being exploited by hackers and cybercriminals and instruction on how to recognize and avoid them. This will empower

K Financial, Inc.

The State
Mercantile Building
801 Main Street, Suite 225
Louisville, CO 80027
Phone: 303.665.8060
Fax: 303.665.0813
www.kfinancial.com

employees to be the first line of defense against hackers and reduce the risk of being hacked. Security awareness training is arguably one of the most valuable investments that companies can make.

Thanks for reading!