Andree Salvo

Southern New Hampshire University

CYB 400 - 6-2 Activity: Understanding Third-Party Audits

Instructor: Robert Chubbuck

To: Sarah Jackson, Director of Information Services

From: Andree Salvo, Security Analyst

Subject: Justification for Third-Party Security Audit

Dear Sarah,

I am reaching out to discuss your support in conducting an independent audit following the BrainMeld acquisition and to convey insights from the case study we have examined this week. Drawing on the conclusions and lessons of the case, I strongly advise that Grey Matter must proceed with a third-party security audit.

For 20 years, the company has never undergone a third-party audit review, relying heavily on the internal teams. An external audit would benefit from an unbiased assessment of our security measures. This is particularly important with the integration of BrainMeld, which can introduce new systems, data, and potential risks. A third-party audit review would help with compliance, catch any overlooked vulnerabilities, and build trust with our clients and stakeholders in the long run.

Even though internal teams are great experts in their fields, they can sometimes miss things because they're familiar with the systems and processes. Third-party auditors come into play because they offer valuable insights and introduce best practices from across the industry. They

often spot vulnerabilities that internal staff might overlook, either because of routine assumptions or a limited scope of view.

The audit in the case study proved its worth by uncovering issues that the internal team was unaware of, such as null passwords, default SNMP configurations, and a web vulnerability that exposed database credentials. However, it identified a significant compliance problem involving the improper sharing and storage of sensitive data. With these issues, the security team addressed the vulnerabilities, enhanced password and patching protocols, and secured data transfers through encryption. Moreover, the organization established policies and training programs that fostered a stronger security culture for the future. In essence, the audit not only identified weaknesses but also directly made improvements that enhanced the organization's security and compliance requirements.

The Agency from the case study demonstrated that internal diligence was insufficient, and that written policies, user education, and ongoing monitoring were critical to sustaining improvements. With a limited budget, they were able to strengthen compliance and build a culture of security. If we adopt a similar approach, a third-party audit can serve not only as a compliance measure but also as a foundation for lasting improvements throughout our organization.

I am fully supportive of proceeding with this initiative. By acting now, we can identify potential vulnerabilities, strengthen our protective measures, and reaffirm Grey Matter's unwavering commitment to security and trust. I am grateful for your leadership in bringing this significant issue to light.

Best Regards,
Andree Salvo, Security Analyst