COSMOS®
Navigate the Compliance Universe

Report on Supply Chain Compliance Volume 2, Number 15. August 15, 2019
Recent data breaches have compliance professionals asking, ‘What can I do better?’

By Sascha Matuszak

The recently reported Capital One Financial Corporation data breach involves similar cloud computing vulnerabilities discussed in *RSCC’s* July 18 article, “The risk of a data breach to your supply chain is real … and so are the solutions,” namely “S3 buckets,” components of Amazon Web Services (AWS). The Capital One data breach was carried out by a former insider, who had also worked for AWS systems in the past and, according to court documents, was able to take advantage of a misconfiguration of Capital One’s cloud database to gain credentials that allowed access to the personal data of more than 100 million individuals.

Capital One released a statement, including the following:

> We encrypt our data as a standard. In addition, it is our practice to tokenize select sensitive data fields, most notably Social Insurance Numbers and credit card account numbers. Tokenization involves the substitution of the sensitive field with a cryptographically generated replacement. The method and keys to unlock the tokenized fields are different from those used to encrypt the data. Due to the particular circumstances of this incident, the unauthorized access also enabled the decrypting of the data.

According to Mark Lanterman, chief technology officer of Computer Forensic Services, the breach had little to do with encryption issues:

> I believe, based upon [alleged hacker Paige] Thompson’s own comments, that the data was encrypted at some point. But encryption isn’t a silver bullet. If an attacker gains access to system rights, which occurred here, encryption becomes trivial. Think of it like this — the data on your iPhone is encrypted, but if someone is able to get the password, what good is that encryption to you? This breach was less about encryption and more about access controls.

A pervasive problem

Every major organization in the world is using cloud computing to store data and conduct business operations. Cloud computing carries its own particular cybersecurity risks, and given the recent high-profile fines levied against British Airways and Marriot International Inc., and the breach at Capital One, it’s critical that compliance officers understand the nature of cloud computing risks and how to mitigate and prevent costly breaches.

The Wall Street Journal reported that the U.S. Federal Reserve conducted a brief inspection of Amazon’s cloud computing facilities as part of an effort to start regulating an industry that has intertwined itself into every facet of the economy, especially banking and finance.

“Technology companies such as Amazon are now a crucial player in the U.S. banking system, whether they want to be or not," the article stated. "They run the databases that hold customer credit scores and social-security numbers. They analyze risk for banks' traders and process payments. Cloud computing has made possible services that customers now take for granted, like mobile access to their bank accounts and split-second decisions on their efforts to buy and sell securities."

Supply chains are increasingly dependent on cloud computing to manage all manner of data and transactions, not just financial data. Purchasing information, vendor management data, data related to mandatory disclosures, sanctions, Harmonized Tariff Schedule codes and classifications, restricted substances, and information regarding investigations that auditing companies have done are all examples of data being stored in the cloud. Establishing proper security procedures and data breach response protocols is critical to maintaining business continuity.

The Capital One data security team was referred to in the media as one of the strongest in the corporate world and was even featured on the AWS homepage as a case study. Nevertheless, Capital One suffered a severe data breach. For many other organizations out there, this breach and the many before it should serve as wake-up calls.

Don't 'do it wrong'

For organizations seeking guidance and advice, particularly when it comes to cloud computing, there are resources available. One great resource is the "Security Guidance for Critical Areas of Focus in Cloud Computing v4.0," put together by the Cloud Security Alliance, a not-for-profit organization with a mission to "promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing." The guidance is organized into 14 domains covering everything from basic definitions and concepts to audit management, regulatory compliance, encryption, and incident response.

Another good resource is SecureWorld, an association that puts on conferences and training sessions for a network of IT industry experts, thought leaders, practitioners and solution providers. They hosted a webinar, "Cloudy with a Chance of Breach," that provides expert insight into the risks of cloud computing, as well as solutions and strategies for protecting cloud data.

With the AWS vulnerabilities that seem to be the common thread linking the recent data breaches, simply following the latest code developments and ensuring that everything is updated and configured properly goes a long way to keeping data secure. The alleged hacker involved in the Capital One case, Paige Thompson, was quoted as saying that everyone is "doing it wrong," in terms of keeping their software updated and tight. A lot of this also comes down to following cybersecurity trends and experts, staying informed and performing regular audits. Many of the exploits have patches and solutions already available.

Employee training can also help even the odds against very sophisticated and highly skilled hackers, who spend every working day seeking exploits.

"If someone were to appear in the corporate headquarters without a badge, that person wouldn't get very far without being reported to security," said Jonathan Armstrong, partner at Cordery Compliance Ltd., a consulting firm that specializes in data security. "The same should be the case for online intrusions."

Takeaways

- Cloud computing is taking hold across all sectors and industries. Ensuring data is stored securely on the cloud requires specific protocols and procedures that every compliance officer and their IT counterparts should be aware of.
- Several recent data breaches compromising the data of millions of individuals involved vulnerabilities for

which solutions and patches already exist. Routine maintenance and updates can go a long way in securing data.