WHAT ARE THE SUPPLY CHAIN TECHNOLOGY TAKEAWAYS OF THE CAPITAL ONE DATA BREACH INCIDENT

August 8th, 2019 • Supply Chain Matters • Bob Ferrari

By now, many of our Supply Chain Matters have read general media stories about the data security breach involving Capital One bank that was exposed in late July. This incident has been described as one of the largest data breaches to-date, and one of the largest data thefts involving a bank.Capital One Bank

The hacker reportedly gained access to upwards of 100 million consumer credit card applications, 140,000 U.S. Social Security numbers, one million Canadian Social Insurance numbers, and 80,000 bank account numbers, all dating back to 2005.

Some of this data was "tokenized," meaning that the hacker needed access to the API's that converted the data to readable text.

The alleged and now arrested and charged hacker, was a former employee of Amazon Web Services (AWS), that hosted the Capital One data and applications in the Cloud. She reportedly was an organizer of an online social network group with a shared interest in distributed systems, "hacking and cracking." The hacker actually boasted online of: "dropping capital one's dox and admitting it" which led to eventual arrest and charging.

Capital One has since indicated that based on internal analysis, the bank believes that the information was unlikely used for fraud or disseminated. Such a statement will not place eventual impacted consumers at-ease, nor assuage customer concerns about the robustness of the bank's ongoing cyber security and data protection measures.

Our purpose in this blog is to highlight what this latest incident implies for multi-industry supply chain management teams and IT professionals supporting such teams.

Situational Perspective

Included in our Ferrari Consulting and Research Group's 2019 Predictions for Industry and Global Chains (Available for complimentary downloading in this website's Research Center), we were compelled to predict that cyber-risk and information security safeguarding are now a mandatory requirement for any business and its associated supply chain data and information. The need stems from both inevitable risk, and from increasing mandates from stockholders, boards and C-Suite executives who rightfully are now more attuned to the consequences of such attacks.

Supply Chain Matters has additionally featured periodic updates on cyber and data security threats, highlighting three specific vulnerability themes, and now adding an additional theme:

Data Security Lapses

This area has involved the constant threat of unintended data security lapses by internal or Cloud provider IT support teams in patching system vulnerabilities in a time sensitive manner, or in

SUPPLY CHAIN MATTERS

Vormittag Associates, Inc.
A Leader in Enterprise Management Software
www.vai.net

system users in compromising login information.

In a prior commentary, we observed that threats can be from both an inside-out, or outside-in perspectives, the latter often related to extended supply chain B2B systems. If incidents such as the Capital One breach can happen to banks, who have multi-million-dollar data security budgets, they can happen to any business.

Specific identities for all users coupled with constantly monitored specific access, and provisioning inactive employee accounts to certain data are becoming essential.

Disgruntled Ex-Employees

Significant prior incidents have often exhibited an underlying threat of former or disgruntled employees who leave their employers with detailed knowledge of existing systems that may include certain user logins, known data security vulnerabilities or penetration points.

In the Capital One incident, the alleged hacker was a former software engineer once employed by Cloud infrastructure provider Amazon Web Services (AWS), who hosts some of this bank's public Cloud systems. The hacker had an online identity of "erratic" and often boasted on efforts to penetrate major systems. It was that boasting that led federal investigators to be able to specifically identify this person. An FBI report indicated in court papers that the hacker gained access via a "misconfiguration" of a firewall on a web-based application, allowing communication to occur with the server and the eventual stealing of sensitive information.

Need for Active Supply Chain Wide Defenses

Our third consistent theme has been the need for active supply chain wide cyber-security measures supporting both internal behind the firewall and external Cloud based systems.

In conjunction with this blog commentary, this Editor had the opportunity to speak directly with Kevin Beasley, CIO at ERP applications provider VAI. This is a provider who was hosted their own Cloud based infrastructure for over 10 years.

Beasley categorized the Capital One breach as dark web, as contrasted with a state-sponsored attack, with the ex-employee theme. He questioned why such sensitive data was housed on the Public Cloud and surmised that the alleged hacker had knowledge or gained access to the API code that related to unlocking the data token to expose that data. He pointed out that according to reports, it was an outside party that alerted Capital One to the potential breach, based on the hacker's online social postings. That implies that the bank was unaware of the intrusion for some time period.

Some Cloud technology platform or database providers have been introducing artificial intelligence-based machine learning capabilities to automatically detect when an intrusion has occurred. Database providers IBM and Oracle have each introduced technology for this purpose. In its attendance at last year's Oracle OpenWorld customer conference, Supply Chain Matters profiled the introduction of Oracle's autonomous data security support capabilities. The capability introduced was a recognition that bad actors are increasingly far more sophisticated in their cyber-attacks, and that no single business can hire enough cyber experts to protect itself from attacks.

Added Dimension- Functional vs. IT Goal Conflicts

In our interview discussion, we speculated that the bank's decision to house such sensitive data on a Public Cloud might have

been marketing or line-of business motivated, perhaps a means to offer banking customers the ability to complete banking applications online. Such business process related decisions often come with tight deadlines to get prototypes up and running quickly, with the assumption that data security needs will be addressed later.

In some cases, it can be human error, or an assumption that the Cloud hosting provider would take care of security. Perhaps our supply chain or line-of-business readers can relate to such goal conflicts, the need for introducing new web-based functionality in a market sensitive timeline without having the time to address broader requirements in areas such as ongoing data security.

Beasley urged us to share on this blog the importance of resolving time-critical business process decisions with the critical importance of adherence to cyber and data security defenses. That includes not only program implementation measures but annual security audits and tests. Effort to get Cloud-based prototype processes up and running quickly must factor the reality that the threat of cyber attacks are becoming inevitable. Partner with and maintain a constant dialogue with internal IT teams on cyber defenses and actions. IT has responsibility to ensure that such defenses and actions protect the business and its associated customers.

Take Away Summary

In short, the implication for multi-industry supply chain management teams is that the increased frequency and magnitude of cyber attacks and intrusions must remain a heightened concern. It includes companies large and small with complex supply chain networks that generate sensitive data among multiple internal and external systems.

The Capital One data breach incident provides yet another acute reminder and learning of the changing scope of threats.

Time-to-market pressures have to be balanced with cyber defenses. Internal and externally hosted Cloud systems need to adhere to constant monitoring and active data protection defenses.