Vendor Employees Gone Wild: Structuring Vendor Contracts To Guard Against Rogue Insiders & Cyber Threats

August 1, 2019 – Michael Berman, Founder & CEO – Ncontracts

Capital One and its credit card applicants and customers haven't had the best year.

Earlier this year the Virginia-based bank announced that a former Amazon Web Services employee hacked into one of its databases and accessed the data of 100 million Americans and 6 million Canadians, which includes names, addresses, zip codes/postal codes, phone numbers, email addresses, birthdates, income, credit scores, and payment history.

Capital One expects the breach will cost the bank between $100 and $150 million, including customer notifications, credit monitoring, and legal costs.

It's not just the size of the breach or the fact that the "oversharing" hacker enjoyed bragging about her data heist publicly online that's got tongues wagging. It's also the Amazon connection.

Paige Thompson, the 33-year-old arrested and charged with computer fraud and abuse, worked as an engineer for Amazon in 2015 and 2016 in the same web services division where Capital One's database was hosted. Capital One noted that "a highly sophisticated individual was able to exploit a specific configuration vulnerability in our infrastructure" that Capitol One had built for Amazon to host. Capital One has since remedied the vulnerability.

Did inside knowledge of Amazon aid Thompson in accessing Capital One's data? Amazon says no, and that Thompson used information anyone could have uncovered, according to news reports.

Yet this situation raises important concerns about third-party vendors' employees. Employees of critical vendors have access to financial institutions' sensitive data and the systems that protect them. They play an important role in safeguarding data and are just as capable of causing a data breach as a financial institution's own employees. It's not just about behaving ethically—though that's a big part of it. It's also avoiding phishing and social engineering schemes that could introduce malware, ransomware, and other threats.

Best Practices for Vendor Employee Data Access

One of the most effective ways to guard against the threat of third-party vendor employees leveraging their inside knowledge and access to steal sensitive data is through a carefully written third-party vendor contract. That includes provisions that ensure vendors are following best practices for IT security and have strong controls, especially when it comes to employee data access.

The contract should ensure vendors have policies and procedures that require them to:

- **Limit access to data and keep careful records of who has it.** Not every employee needs access to your sensitive information. Vendor policies should require the maintenance of an accurate inventory of all employees granted data access. Those who leave the company or switch to a new project and no longer require data access should lose their credentials. Regular audits should ensure that every person on that list needs that access to do his job. This may seem like a basic tenet of IT security, but you'd be amazed how often a company forgets to cut off access. Though inappropriate access doesn't appear to be a factor in the Capital One breach, it can easily play a role in other breaches.
- **Encrypt data.** If possible, vendors should encrypt data so that even if someone gains access to it, they can't decipher it. Encryption and tokenization shielded Social Security numbers from Capitol One's hacker, slightly limiting the scope of the breach.
- **Conduct penetration testing.** The purpose of penetration testing isn't just to see if outsiders can get in. It should also assess whether people with system access can get into areas they shouldn't. Employees often know the quirks and vulnerabilities in a system.
- **Follow the audit trail.** Logs should keep track of who accessed what data and when. These logs should also be reviewed for anomalies. While Capital One was able the confirm the breach through its logs, it only found out about the breach due to an anonymous email from an outside source three months after the breach occurred. A review of the logs could have caught the breach sooner.

Using the Contract to Limit Risk of Vendor Employee-Caused Data Breaches

Contracts can also ensure vendors are hiring and training employees who respect data security principles and help weed out potential bad actors.

Contracts should require vendors to:

- **Regularly perform background checks on their employees.** Make sure the term "background check" is clearly defined. It may include criminal records, terror watch list, credit reports, drug testing, or professional license verification. Also define "regular," and whether it's once a year, once every three years or some other period.

It's not enough just to conduct background checks upon hiring. Circumstances change. If someone had been looking to hire the Capital One hacker over the last month or so and done a social media search, he would have might have discovered she was engaged in criminal hacking.

- **Mandate security awareness training for vendor employees.** Employees need to be aware of the company's policies and procedures on security and compliance. Details make for a stronger control. Determine how often training will be conducted, what form it will take, and how it will be audited. Employees who know there are strong controls may be less likely to try to exploit vulnerabilities.
- **Training on the legal ramifications of handling data.** Employees should be made aware of relevant state, federal, and international data breach laws and regulations and the consequences of violating them. Determine if the vendor requires employees to sign secrecy, confidentiality, or nondisclosure agreements to protect your data. Find out how often this information will be reviewed. Signing a legal document and knowing the consequences for illegal actions can be a deterrent to misbehavior.
- **Carry adequate cyber insurance.** A company typically is responsible for the actions (or inactions) of its employees. Require your vendors to be insured in the event of a data breach. This way if one of its employees is responsible for a breach, your FI is in the best position to be compensated for the expense of remediation.

Vendor Management to the Rescue

Beyond contracts, vendor management offers other tools to guard against the risk of vendor employees (and former employees) deliberately or accidentally breaching sensitive data. It can help uncover systemic problems or issues that need to be addressed.

These activities include:

- **Reviewing reports and audits.** A well-written contract can ensure FIs receive reports documenting vendor IT security and training, but they won't do an institution any good if they aren't reviewed. Make sure someone experienced reviews any documentation received to make sure the vendor (and by proxy its staff) is living up to its promises.
- **Real-time vendor monitoring.** As part of ongoing due diligence, make sure your institution constantly reviews any vendor-related lawsuits, government proceedings, news headlines, and complaints for potential issues or weaknesses in employee and IT controls. The Capital One data breach made national news, but smaller breaches might not.

Preparing for the Worst Case

In the event a control fails and a data breach occurs, make sure your institution can handle the financial hit. The global average cost of a data breach is $148 per lost or stolen record and costs $3.86 million, according to a report by Ponemon Institute. In the case of the Equifax breach, it's $700 million.

Understand your institution’s cyber insurance policy and whether it includes third-party breaches. General liability or business interruption policy may not cover cyber events. Review your current insurance coverage to understand what is and isn’t covered. Cyber insurance can be purchased as standalone coverage or as a rider to an existing policy.

Don’t put off protecting your institution from errant vendor employees.

Make sure proper vendor management has you covered from A to Z.

###

About Ncontracts

Ncontracts® is a leading provider of risk and compliance management software and services to financial institutions. While we started with our industry-leading vendor management platform, our portfolio offerings have evolved to feature enterprise risk management, business continuity planning, audit and exam findings management, contracts management, lending compliance and compliance management system. More than 1,400 financial institutions use Ncontracts to manage risk and compliance more efficiently and effectively using our integrated suite of software and services.

With Ncontracts, your organization can be empowered to enjoy the upside of risk.