When Ghosts are Good: Basic Cyber Security Practices

With more than half of all small businesses likely to experience some form of data breach over the course of their existence, learning a few basic cyber security practices is not only useful, it can save time, money, and heartache in the long term. David Rains relates a couple of these hard-earned lessons from his own experience and reflects on why ghosts aren't always so scary.

BY DAVID RAINS

At a time when 55 percent of all small businesses will experience a data breach,* data security is top of mind for most of us. We typically think about external hack attacks first, but we must also remain vigilant for insider breaches that can blindside us. Let me share what happened to my company as a cautionary tale for your business.

SITUATION

An executive vice president of our company, a long-time trusted employee, was untruthful about his work performance. After unsuccessfully working with him for several months to meet company performance standards, he was fired for cause. The second he was fired, his login credentials were terminated.

DISCOVERY

The former employee then began working as a consultant for another firm in Arizona. Soon after, I received a solicitation e-mail to my ghost e-mail address from the former employee under the banner of the new company he'd joined. The ghost e-mail account was a fictional contact embedded in my company's

*https://www.nationwide.com/what-is-cyber-insurance.jsp

database, created to detect data breaches and to quality test e-mail campaigns. On receiving the e-mail, I immediately suspected a database breach and, given the timing, suspected the former employee was either directly responsible for or knowledgeable about the matter.

You can imagine my shock when we later discovered in litigation with the former employee that when we were working to try and help him improve his work performance, he had made an agreement with another ex-employee who had previously done database work for the company and therefore knew how to access our company's data through the SQL back door. By working with this individual, the former employee was able to obtain a copy of the company's database, as well as download and export over 11,000 documents.

RESPONSE

On receiving the ghost e-mail, I immediately called our database hosting company to determine how the breach had occurred, as nothing showed up in our server history. They confirmed that our database was accessed through the company's SQL bench on two occasions, each using the former employee's login credentials. The company had left the SQL socket open because some businesses use it for database management, and we had never specifically asked them to close it since we had started working with them. We sent notice to promptly close the socket and, through litigation efforts, obtained a temporary restraining order against the former employee, prohibiting him (and the new company he'd joined) from using the company's data. Through a several-year legal process, we eventually obtained a permanent injunction and a money judgment in excess of $450,000.

Only three weeks passed between our discovery of the data breach and obtaining the temporary restraining order, a relatively short time. We were fortunate that our data was used only for one e-mail blast. Upon being notified of the data breach, the Arizona company that our former employee had joined worked with us to rectify the situation. They terminated their relationship with him, pledged to never use our data again, returned all copies of our data to us, and deleted our proprietary information from their system. They also paid for the forensic IT experts to examine their server and assure us our data was no longer in their systems, before settling with us in mediation.

The former employee initially lied about taking and using the company's database when confronted, but evidence gathered by the forensic IT experts and database hosting company led to an examination of his laptop computer, whereupon additional confidential files were subsequently identified and removed.

LESSONS LEARNED

1. **Ghosts are good.** Insert a ghost e-mail address, a P.O. box mailing address, a social media profile or even a personal phone number that you own and control into your database; this will allow you to quickly know when your data may have been compromised.
2. **Look inward**. As in factoring, you always must be diligent in detecting bad actors. The same thinking applies even to high-ranking, trusted employees. Limit data access to a need-to-know basis, and find the right balance between convenient, efficient access by employees and privacy.
3. **Think ahead.** When you have an employee who has performance issues, this is a key time to put additional controls in place. Realize they may already be making or, worse, acting upon plans to exit the company. They may be tempted to steal data to hurt your company or to springboard new opportunities.
4. **Close the back door.** As finance people, we rely on and trust our tech experts to mitigate risk. Have a frank conversation with them, and ask who has access and how. Now is the time to learn where your entry points are, not just for your database but across your entire organization.
5. **Dig deep.** Just as large financial institutions and the government hire hackers to try to break into their files to reveal exposures, consider hiring a security firm for penetration testing. The firm may be able to identify hidden vulnerabilities in your organization's networks.
6. **Cover yourself.** A cyber insurance policy can help lessen the sting of the costs you incur in the case of a breach, including legal costs, forensics, security audits, and credit monitoring.

In the end, our former employee was convicted of a third-degree felony and required to pay restitution in addition to the aforementioned civil remedies, but the company went through an expensive, arduous two-year legal process that drained resources and absorbed valuable time in order to get there. I hope sharing our case will help prevent this from happening to others. •

David Rains is the founder and president of Commercial Finance Consultants and FactorHelp. In the past 20 years, CFC has placed over 14% of the ABL and factoring industry while FactorHelp has been instrumental in helping over 50 startups enter the industry. David may be reached at dar@searchcf.com or at his office at 469-402-4000.