Innovative Computing Systems

Los Angeles | San Francisco | Austin

ARTICLE

After the Attack — Eight Steps to Take Immediately Following a Law Firm Data Breach

By William Pate

It has happened. You have done everything you can to defend your law firm from this day, but a hacker has successfully breached your walls. Now, you are faced with your client files being encrypted and inaccessible, lost confidential data, demands for money, the insertion of other forms of malware on your network or, even worse, some combination of these or more malicious activities or demands that you cannot identify.

What do you do right now? Follow these eight steps immediately after the cyberattack:

Step 1: Isolate the Infection

The first thing to do is to isolate the affected endpoints and servers. These should be disconnected from all other systems to prevent the malware from spreading. Do not shut the machines down until your information security experts have examined them. In the case of a ransomware attack, your first instinct may be to reload the data from backups. However, doing so without first implementing updated security solutions could result in your backups becoming infected too.

Step 2: Call IT Security Professionals

After a significant breach, organizations should retain information technology security professionals with expertise in security well beyond just systems administration. Attempting to remediate a security breach without securing highly experienced professionals may be inefficient, and potentially inadequate. A third-party audit of your systems should be strongly considered.

Step 3: Notify Authorities

There are a number of organizations and agencies you should contact following a cyberattack.

1. Let your local police department know so the attack can be made official and a paper trail initiated.

2. The agency you often hear the most about is the Federal Bureau of Investigation. You'll want to get in touch with the FBI Internet Crime Complaint Center *(www.fbi.gov/investigate/cyber and www.ics3.gov)*.

3. The Secret Service does more than protect the president. They also have an Electronic Crimes Task Force where cyberattacks can be reported *(www.secretservice.gov)*.

4. The U.S. Computer Emergency Readiness Team (US-CERT) out of the Department of Homeland Security is another important organization to contact *(www.us-cert.gov)*.

5. You should also file a complaint with the Federal Trade Commission. If confidential or personally identifiable information has been compromised, ensure your clients visit the Federal Trade Commission's Identity Theft site *(www.ftc.gov* and *www.identitytheft.gov)*.

Step 4: Inform Clients

Among the most difficult steps post-attack is contacting and explaining the situation to your clients. While an organization may be reluctant to share that their defenses have been breached, it is of utmost importance that your clients be informed so they can take appropriate measures to protect themselves and their families. Engage with your clients, vendors and other partners with an eye to your legal and regulatory requirements. You should review your responsibilities with legal counsel.

Step 5: Identify Vulnerabilities

The third-party security professionals you hired can help identify and mitigate the vulnerabilities used to illegally access your network. Further, they will often find other vulnerabilities that must be patched. While no network is impenetrable, by performing due diligence and layering security — what we call implementing defense-in-depth — on your information security infrastructure, your firm will be as protected as possible.

Step 6: Deploy Security Solutions

In the wake of a successful attack, it has become clear that your current information security solutions are not sufficient. Once your vulnerabilities have been identified, deploy security software, hardware, protocols and training to strengthen your organization's cybersecurity. Use a defense-in-depth approach by layering your security with endpoint protection, anti-virus, firewalls and other defenses.

Step 7: Develop an After-Action Report

What happened? How did you recover? What did you learn? Answer these and other questions about the incident, its consequences, the changes you have made in response to the attack and compile them into a document that can be shared firmwide. It is important that employees know where the attack originated, what its effects on the firm were, how to avoid it in the future and what the firm has done to increase security.

Step 8: Refresh Your Training

No matter how the hacker got into your network — whether it was an employee's errant click on an infected email or dumb luck in guessing a password — it is time to refresh your employees' cybersecurity awareness. Use your after-action report and be sure to teach your employees how to identify and appropriately respond to cyberattacks — whether they were successful or unsuccessful. Oftentimes, the human is the weakest link in the information security chain.

Cybersecurity is not just hardware and software. It is also about knowledge, and information-sharing is important in building that knowledge base. When your law firm or organization is attacked, share the information to get help and protect others.

About Innovative Computing Systems, Inc.

Since 1989, Innovative Computing Systems has primarily focused on the technology needs of law firms and legal departments. Innovative Computing Systems skills are also sought out by entities such as municipalities, corporate environments and professional services industries. Innovative Computing Systems takes a best-of-breed approach to all its offerings by selecting only premier technology partners to provide solutions for our clients. We are committed to maintaining long-term strategic relationships with clients to ensure the highest levels of success with IT initiatives. Learn more by visiting www.innovativecomp.com.