How to Survive a Data Breach

Zdenêk Valach

A PEO is a virtual treasure chest of personally identifiable information (PII). One errant email attachment or one stolen laptop can force a PEO into a fight to save its reputation. For example, take these two possible scenarios:

- Scenario Number 1. The client of a PEO requests a report that includes employee Social Security numbers (SSNs) and bank account numbers. It is the end of a long day. The payroll specialist creates the report, addresses the email, and hits send. Worst of all, she forgets company policy and fails to encrypt the data. The next morning, the client writes, "I'm still waiting for that report."
- Scenario Number 2. A PEO vice president is on a business trip. He takes a client to dinner. When he returns to his hotel room, he finds that his company computer has been stolen. He immediately reports it to a colleague back home. They try to log onto their payroll software with his credentials. The password has already been changed.

Just like that, every Social Security number, every driver's license number, every bank account number, every birthdate, and every phone number is out in cyberspace. These scenarios are merely two examples of what can go wrong for a PEO.

In both scenarios, it is imperative to react quickly.

- What if dozens of worksite employees use a community computer for logging in and adjusting personal benefit plans during open enrollment? Is the personal information secure? Does each employee properly log off?
- What if an insider steals personal information and sells it on the black market?
- What if a microprocessor flaw allows a hacker unimpeded access to your payroll system?

We have all seen the articles about what a PEO should do to increase its security: demand unique passwords, enforce proper procedures, use certified and secure software, maintain the latest databases, and obtain data breach insurance. It is the cost of doing business. Bloomberg Technology expects that worldwide spending on security-related hardware, software, and services will jump from $73.7 billion in 2016 to near $90 billion in 2018.[1] Yet, nobody will feel 100 percent safe. Nor should they.

What should you do if your PEO or a client has been the victim of a data breach?

A Step by Step Guide to Dealing with a Data Breach

If you do not have a data breach response/disaster recovery plan, now is the time to create, test, and implement one. You can search for the many resources available that provide basic templates to assist with this task, or you can partner with a data breach resolution advisor.

Secure the crime scene.

If you have lost control of data or if your system has been hacked, then a crime

1 *www.bloomberg.com/news/articles/2017-01-19/data-breaches-hit-record-in-2016-as-dnc-wendy-s-co-hacked.*

has likely been committed. Contact your Health Insurance Portability and Accountability Act (HIPAA) security officer or designated internal resource. Call the local police department. You may also need to contact the FBI or the U.S. Secret Service.

Secure your system as well as you can. Take infected equipment offline. Seal off undisturbed servers. Make sure that no records are deleted or clues are lost. Restrict access to essential personnel. Change access codes and passwords.

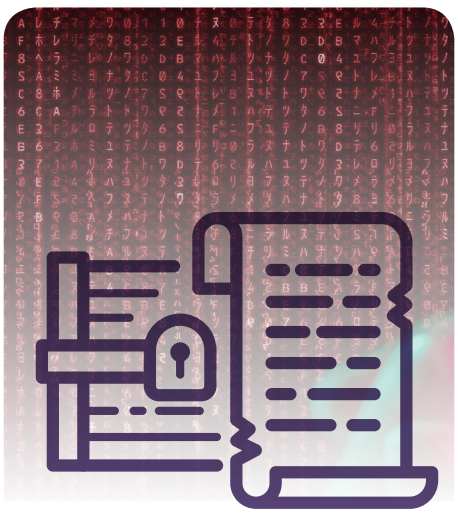
Interview the people who identified the breach. Establish a timeline: How long has the information been compromised? Who was online at the time? Consider hiring a forensics expert to thoroughly assess the damage.

Contact principals.
Contact people up and down the organization chart. It's all-hands-on-deck and support is imperative. Top management needs to make decisions. Legal counsel should be consulted to advise on state and federal regulations, disclosures, and documentation. Someone in the IT department may have useful institutional knowledge. Marketing and customer relations should be notified. Contact your cybersecurity insurance provider.

Get back online.
Implement your company's disaster recovery plan. Control the damage to get the provisional functions operating so you can get back online as quickly as possible. Time is money. A segmented network, which has built-in redundancy, may make it relatively easy to seal off the infected part of the system and continue normal operations with clean machines.

Release information.
There are many parties who should be informed. The authorities are first in line, and, given the active crime scene, there may be some considerations for notifying clients, worksite employees, and the general public. Use legal counsel to check your state and federal laws for regulations and specific requirements for your business.

- Credit agencies. If names and Social Security numbers were stolen, contact the major credit bureaus and warn them to expect an influx of fraud alert requests and credit freezes.
  - » Equifax: *www.equifax.com* or 800/525-6285
  - » Experian: *www.experian.com* or 888/397-3742
  - » TransUnion: *www.transunion.com* or 800/680-7289
- Electronic health information. If the data breach affects health data, you may be required to contact the Federal Trade Commission (FTC) or the U.S. Department of Health and Human Services.
- Financial institutions. If credit cards or bank accounts were compromised, notify the respective banks and credit unions to monitor for fraudulent activity.
- Notify clients. Once you know the extent of the breach, plan your strategy for dealing with the aftermath among your clients. Is only one affected? Might others soon show signs of compromise? Err on the safe side to keep a bad situation from getting worse. Issue an internal memorandum advising employees how to respond to client inquiries.
- Notify individuals. Make sure that worksite employees and perhaps even the public know that their personal information was compromised. Suggest fraud alerts and credit freezes. Be consistent and transparent. Base everything on facts. Consider hiring a public relations firm.



Maintain communication.
Stay in touch with your clients, worksite employees, and the public. Explain how you will contact them in the future—by mail, email, or a dedicated section of your website. Provide up-to-date information and descriptions of the steps you have taken and the steps they should take. If there is any good news from the investigation, share it. Regular communication goes a long way toward retaining clients.

Be prepared for lawsuits.
Keep your legal counsel close. Big companies are feeling the pressure for not responding promptly and effectively to data breaches: Uber is facing several lawsuits because it concealed a data breach of 57 million customers and drivers for more than a year, and reportedly paid a $100,000 ransom. Even a professional data breach response plan may not be enough to satisfy everyone. PEOs and their clients must also be prepared for potential litigation.

Conclusion

It is hard to know the severity of data breaches. In our initial scenario, the payroll specialist got lucky—the misaddressed email with the unencrypted data was located and destroyed. In the second scenario, the stolen laptop and the changed password were clear signs that the software was compromised. Quick implementation of the company's data breach response plan limited the damage.

A small slip-up can lead to a catastrophic problem that could be costly in dollars, in clients, and in reputation. Adjust these steps to your PEO to adequately protect your business.

Expert help to create a professional data breach response plan is worth the investment. For more details, go to the Federal Trade Commission website at *https://business.ftc.gov* or the Better Business Bureau site at *www.bbb.org/council/for-businesses/cybersecurity*. ●

Zdeněk Valach is chief technology officer for Worklio's Brno, Czech Republic, office. Worklio is headquartered in Miami, Florida.