E Com Security Solutions

What to Do If You Have a Security Breach in Your Data Center?

"In today's environment, it's not a matter of if a data breach will occur, but when it will occur, and how well you respond. Do everything you can to prevent data breaches, but also fully plan out how you will respond if you are breached. Today's media and business environment demands that two-pronged approach."

1. Evaluate the Situation

Is the event over? What's the damage? What data is affected? If additional loss or damage is imminent, you must consider taking IT assets / servers off-line

2. Preserve the environment

And even if there's not a sufficient criminal case, computer forensics personnel can gather evidence to possibly identify perpetrators or means of attack, enabling improvement of the security system.

We suggest leaving on all servers, as shutting them down can destroy information that may be critical to an internal or criminal investigation. Document what you do and create chain of custody records. Speed can be important, as the shelf life of digital evidence is often short.

In a post-event world, you will inevitably need to have the ability to identify the important critical first steps taken after a breach was discovered. Error on the side of over documentation.

Keep track of IT assets, the times and dates of key events, records of which response team members were notified and when, etc.

3. Notify the Team.

Your response protocol should include a collaborative team of professionals from Legal, IT, HR, Corporate Security, PR, Insurance Claims, and outside computer forensics experts. Make sure you have team contact information (and alternative contacts as back-ups).

Also consider your regulatory reporting requirements as time limits sometimes exist for the reporting of data breaches.

4. Notify affected parties.

You may need to inform affected parties regarding the data breach, particularly if it involves medical or financial records. Here, consulting with an attorney or compliance officer will help you take the right steps to avoid fines and lawsuits. Honesty may not be pleasant, but it may be the required policy in the wake of a security breach.

5. Address legal and regulatory issues.

If your data center handles financial or medical data, then PCI DSS, HIPAA or other compliance issues will come into play. Data breaches involving medical records can be

very costly, but you still may need to inform the appropriate regulatory agencies. Also, consult with your legal team or an outside attorney regarding any implications of the breach. Legal counsel can help you avoid costly mistakes in resolving the breach.

6. Evaluate your staff's performance in response to the breach.

Practicing for a security breach is one thing; responding to an actual breach is another. Look at how your team did in response to the breach. Certainly, don't be too harsh: mistakes will almost certainly be made. Take a constructive approach that seeks improvement, not laying of blame. Of course, the hope is that you'll never again have to practice the skills you learn for dealing with security breaches, but chances are if you're in business long enough, it will happen again. Modify your plan so that next time, you'll be even better prepared to deal with the situation.

7. Identify the weakness in your security system and take steps to strengthen it

Remote Access Termination, in cases involving the loss or theft of portable confidential information, such as trade secrets stored on an iPhone, don't forget to terminate the user's remote access / VPN accounts to prevent unauthorized access into your network. Even better, make sure the data on portable devices (especially laptops) is encrypted to minimize data compromise.

Hackers and other malicious parties spend a lot of time trying to break into systems like yours. Some breaches occur despite the best efforts of companies to secure their data centers—the only shame is in not taking the necessary steps to resolve known weaknesses.