What should you do if your network or email is compromised?

Every day we receive a note from a candidate or a friend that their email has been hijacked or worse an email from the hijacker trying to sell us something

In June 6.3 million passwords were reported stolen when a hacker was able to access LinkedIn's servers. The news made headlines and everyone was talking about it. Clearly this is a public-relations nightmare for LinkedIn and that will, have a ripple effect for possibly years, as they deal with the fallout from their clients and potential lawsuits.

What's scary about this type of attack- or any major security breach- is that if I can happen to them, it can certainly happen to YOU! Although we are not privy to LinkedIn's security procedures, I'm sure they don't take it likely and most likely invested a major amount of money to keep their data secure, money that the "average" small hotel or business owner could never afford to spend. So IF this happened to your company, what should you do? How do you avoid the loss of both sales and the trust of your guests, and even potential lawsuits?

The first step would be to identify the type of attack it is and what machine(s) were affected so you can quickly contain the damage done (or being done) as best as possible and protect your assets. Naturally, you should consult with a professional security expert to make this containment happen as quickly as possible to "stop the bleeding."

Next you'll want to notify any and all parties affected as fast as possible. In the LinkedIn attack, they immediately notified the subscribers affected forcing a password reset. The faster you can react to this, the better your changes are of limiting the damage done. We would encourage you to talk to an attorney about the breach and what you need in terms of making a public announcement as quickly as possible– particularly if a security breach exposed your employees, hotel guests, subscribers, or clients to a cyber-criminal. In some cases where medical or financial information is involved, you may be required by law to report the incident not only to your clients, but also to authorities.

By Joe Stoll, President Technical Action Group (TAG) joestoll@technicalactiongroup.com