What to do if your firm gets hacked - and how to prevent it?

You had a nightmare last night. It involved a call from your Information Technology (IT) department informing you they just got notice of a major cyber-attack against your firm. Not much is not known yet, but they fear it is a major attack targeting your customer account information and other sensitive data.

They want to know what to do next. You're the Chief Compliance Officer of a Registered Investment Adviser (RIA) or FINRA Broker-Dealer, and your incident response plan has more dust than value. Your cybersecurity program policy was issued earlier in the year, but it, too, is useless considering it hasn't been implemented let alone tested.

OK, that was a bad dream, but your current reality isn't much better. Getting hacked can be costly and having useless measures will only make the situation worse. Let's see if I can help by providing guidance on: 1) immediate steps to take if your firm has been hacked; 2) preventing and managing cyber-events through a formal program; and 3) applying some best practices.

Immediate Steps

If you had to face a situation like the one you had in your nightmare, what are the immediate steps you can take? Here are some critical immediate steps to consider:

- Assess the situation with your IT folks to confirm a cyber-attack occurred.
    - This assessment will be made much easier if your firm has mapped out cyber-events it can face (phishing, spamming, malware, extortion emails, etc.) and possible scenarios triggering these.
- If you confirm an attack, determine what happened:
    - the source of the attack – internal or external (or both);
    - how the hackers got in;
    - the compromised systems and applications;
    - the accessed or stolen data; and
    - the affected parties (employees, customers, third-parties or business partners).
- Launch a formal internal investigation to gain a fuller understanding of the cyber-event.
- Engage your legal counsel (and if necessary external counsel) to advise you along the way.
- Communicate promptly and clearly to employees, customers, and business partners -- about the attack, what's been done, and what they need to do -- using the appropriate channel (*g*., your website, letter, email, social media, or a full-page ad in a newspaper).
- Check with your legal counsel about what disclosures, if any, must be made to authorities, customers and others, upon discovery and confirmation of an attack.
- Limit the damage of the attack as much as possible with immediate fixes, such as:
    - applying a "patch" from the software vendor;
    - removing infected computers or applications;
    - restoring lost data with clean backups; and
    - requiring new and stronger passwords for compromised accounts.

Now you need to focus on your formal cybersecurity program. Don't set a goal of setting up a program to fully eliminate cyber risk – that's unrealistic. Rather, use the program to help prevent potential attacks and better manage such events in the future. Here's an overview of my 10-step plan to help:

- **STEP 1:** Institute a team of key stakeholders to help in developing, assessing and maintaining the program.
- **STEP 2:** Inventory key information systems and assets and assign each to an owner/custodian.
- **STEP 3:** Establish and maintain a Cybersecurity Program Policy that sets forth principles for the protection of information systems and assets in consideration of any applicable laws and internal operational requirements.
- **STEP 4:** Assess information systems and assets periodically to help identify cyber risks and threats to help determine how the cybersecurity program does or will address the risks.
- **STEP 5:** Operationalize program requirements.
- **STEP 6:** Deliver regular training and use other methods to raise awareness and reinforce

program principles (special roles will require specialist training).
- **STEP 7:** Establish and maintain policies and procedures for managing information maintained, created or used by third-parties, including measures that will be needed to effectively manage these relationships. (**Access Tool**: *Use the sample Incident Response Plan Checklist to assess your incident response procedures and make changes as needed*.)
- **STEP 8:** Maintain a written response plan that identifies: your response team, cyber-event scenarios, appropriate response procedures for investigating, communicating, remediating, and where necessary disclosing cyber-events.
- **STEP 9:** Test program requirements periodically to determine if controls are effective and implemented and that risks are being properly managed.
- **STEP 10:** Keep the program effective and viable by reviewing program components periodically and updating them as needed, as well as providing management and boards with updates.

With your plan and program in place, here are some best practices I want you to keep in mind:

- Make sure that cybersecurity is a top priority for your firm by:
    - getting a commitment from the top down to support the program;
    - have senior management issue communications on the program; and
    - designating a senior officer to oversee your program with unfettered access to management and the board.
- Know the data you have, where it is, its vulnerabilities, who has access, and possible scenarios for breach.
- Test your incident response plan periodically to make sure it is reliable (*g*., excellent scenario forecasting, a well-defined chain of command, response measures, ease of decision-making, communications to affected group, etc.).
- Evaluate the effectiveness of your business continuity plans periodically in the context of assessing cyber-security risks.
- Recruit and retain experienced and capable IT senior executives, and make sure you have a good succession plan to avoid being left short-handed (these folks are in great demand right now).
- Monitor the latest developments in cybersecurity regulations, cyber-event scenarios, and the latest mitigation tools and techniques.
- Keep your employees informed.
- Review your liability insurance policies to determine if your adequately covered for cyber-attack losses. Consider insurance coverage for:
    - Privacy and data breach liability.
    - Computer hardware, software and data damage or loss.
    - Crisis management.
    - Business interruption, denial of service attack and lost income.
    - Loss of business reputation.

- Cyber extortion.
- Media or web content liability.

Conclusion

Regardless of your firm’s size, the degree of cybersecurity risk or cybersecurity sophistication, take steps now. Your efforts will be worthwhile when you face your next cyber-event and can tackle the challenge in a structured way.