5 Steps to Reduce Your Firm's Cyber Risk

Start addressing threats before they strike.

With the increasing number of data breaches, the possibility someone may come after critical information you have stored is real. The good news is you don't have to be a tech genius to tackle this problem. Evaluate and make sure you're doing business in a secure way to best prevent an incident from happening in the first place.

Here are five steps to get you started:

1. Create Your Own Cyber Security Team

Who on your staff has both a deep knowledge of your business and some technical expertise to boot? Task them with putting safeguards in place.

Endow this individual or team—which may include members of IT or compliance—with the authority to make decisions. Empower them to tighten security and make tough choices on behalf of the firm.

If you don't have the resources or ability to tackle this in-house, look at outside consultants. Hiring a third party for this responsibility may provide better service at a price that's much more reasonable than you may think. (See **"Need Help"**) Keep in mind though that while you can outsource the actual work, you can't outsource the responsibility. Your firm is ultimately responsible for its own risks.

2. Look at What You've Got

Right off the bat, do a complete top-to-bottom risk assessment to ensure the firm conforms to FINRA and SEC guidelines for protecting sensitive customer data.

Ask yourself: What data do you have? Where is it located? Who has access to it and why? You'll need to understand who your major service providers are and where data can be found, whether in the office or on third-party vendors' systems. (If you outsource, confirm they're following proper cybersecurity procedures, as well.)

Once you uncover where you're most vulnerable, begin to formulate solutions. There's no one-size-fits all formula. Each firm will have its own unique items to address. Perform this task at least once a year or when a significant change occurs.

Need Help?

Can't handle cybersecurity in-house? Here's where to turn for help.

1. Your accounting and audit firm. Many of them—especially the Big 4 of Deloitte, PricewaterhouseCoopers, Ernst & Young, and Klynveld Peat Marwick Goerdeler—also have cybersecurity practices.
2. A reputable IT consulting shop (Booz Allen, DXE Technology, Lockheed Martin, HP, IBM, etc.) Check out FINRA's Compliance Vendor Directory's at http://www.finra.org/industry/cvd to search for vendors providing cybersecurity services.

3. Educate Everyone

Cybersecurity is more than just an ongoing part of your annual continuing-education program. Incorporate security-awareness activities and communications throughout the year. Hold firm-wide informational meetings to provide further details of your procedures and policies. Whatever is done in the office should apply to remote workers, too.

Discuss the right ways to store and backup data securely for clients. Start by incorporating this training in onboarding for new hires.

Protecting passwords is a critical first lesson. Never share them. Dual authentication—e.g., receiving a code via text message to use when logging in—creates a safer login environment than a password alone.

Phishing scams are a top way a firm can be compromised. All it takes is one click on a link of a fraudulent email to open the floodgates of malware that can take over a network. Review what a malicious email looks like with your employees.

Do clients put account numbers in emails? Educating your clients on cybersecurity on their end is an important step in closing the loop. Work with them to explain the steps you're taking to ensure their data is safe, and then identify what they can do to prevent opening themselves up to data theft.

Cybersecurity is more than just an ongoing part of your annual continuing-education program.

4. Tighten Up the Ship

Do you have a firewall to block unauthorized access to your computer network? If you answered, "no," then that's your first area to explore for computer protection.

Next, invest in data-loss prevention tools to help you monitor emails when sensitive information (e.g., Social Security numbers, credit card numbers, etc.) is sent. Encrypt this information, too.

Then begin restricting access to only those who require access to different systems or sites that are potential security risks. Require all business to be conducted on work-issued devices, when available. If the members of your firm use personal computers, smartphones, or tablets, have proper security loaded on them. And ensure all antivirus software is up-to-date at all times.

Create a policy of secure procedures for regular business practices—including ways to prevent unauthorized wire transfers or how to encrypt information that is regularly sent.

Your threats may not always come from the digital domain. Protect all data within your organization, whether it's stored in an electronic format or not. Do a physical sweep of the office and check for any confidential paperwork not secured in a locked drawer.

5. Prepare in Advance for a Breach

If something goes wrong, how will you respond? Put a process in place—just in case. Assemble an incident response team. Consider contracting with one or more incident response firms ahead of time. This minimizes unnecessary delays during an actual breach event. By responding in a timely fashion, you'll be able to get back up to full operating capability sooner.

Being on top of an unfortunate incident by contacting clients and partners can often be the key to mitigating any potential damage from a large-scale breach. Test this plan internally. From legal counsel to PR, have the key players ready to help protect your firm's finances and reputation. Do a daily backup of data to have on hand if a system is compromised.

You may also want to explore cybersecurity insurance to help mitigate the financial impact of an adverse event.

If something goes wrong, how will you respond? Put a process in place—just in case.

Be Ever Vigilant

Anyone dealing with personal information is a target for data theft. Cybersecurity must become an underlying business practice. The best time to start thinking about it is before something actually happens.

WPIA003_0220 215907