The True Cost of a Cybersecurity Breach

January 10, 2017

We know it's not the first time you've read a headline like this:

SEC nails advisory firm for cybersecurity failure before data breach:

Firm pays $75,000 to settle charges after approximately 100,000 data records compromised as a result of hack. **(Read the full article here.)**

This isn't the first investment advisory that had to pay the SEC because they failed to have a cybersecurity policy in place and incurred a breach—and it won't be the last. The firm in question paid the fine, but more importantly, their brand became devalued. They had to change their name. And 100,000 of their clients' personal identifiable information was compromised. Let us repeat…their *clients'* data was compromised. If you were faced with a $1M fine, would your advisory be able to stand that financial loss? Even if you could handle the fine, the damage runs deeper. Regardless of what, if any data is compromised, the breach is forever part of your firm. The breach is synonymous with your name.

If your firm's security were breached, would it still have the credibility to remain open for business? Would you still have the clients you've worked so hard to retain? The fact is, it just takes one breach to devalue your brand. So the real takeaway from news like this is: This was not your firm—but it could have been. It's your job to do everything you can to prevent a breach.

That's where we come in.

At RightSize Solutions, we will guide you as you adopt the necessary policies and procedures to safeguard customer information and keep your clients' information—and your firm—safe. Let's talk about how we can help.