Cybersecurity, Cybercrime And Your PR Strategy

By Danny Pehar

In the digitally connected age we live in, our data is everywhere, making it possible for even the likes of the CIA to get hacked. When arguably the most secure organization in the world can be cyber breached, it's safe to say the probability of a cyber breach happening to a regular company is pretty high, and the impacts could be devastating.

Damages to an organization as a result of cybercrime (e.g., loss of revenue, stolen data or money, compliance fines, lawsuits, data restoration services) can be scary, but in my experience of speaking to executives about these very concerns, the biggest fear of a cyber breach is the damage to a company's brand, resulting in a loss of trust with clients, partners and employees.

That being said, if we know there is a high probability of a cyber breach to come our way, and among our main concerns is what that breach will do to our brand, then as we build a strategy of how to respond to that breach, we need to include within that strategy a cyber breach PR plan.

Here are five things to consider for your cyber breach PR plan.

1. Consider Professional Help

Responding to a breach is incredibly important and may have legal complications. Before you respond to anyone, you should consider reaching out to a breach coach. The breach coach will help you respond to legal breach notification requirements that may apply to your business, and they may help you find a PR firm that specializes in breach PR response services. Breach coach services, as well as PR firm breach services, can be covered by a cyber insurance contract.

2. Be Quick To Respond, And Be Sincere

The last thing you want is for your clients to hear from another source about a breach of data they have trusted with you with. Control the narrative by letting them know first with a sincere apology, with details of what has happened and what is being done about it. Not reporting on a breach as soon as you know of

it can not only be incredibly damaging to your brand, but it can have devastatingly expensive fines associated with it.

3. Only Report On What You Know

As important as it is to report quickly, it's equally as important to report accurately. Making claims you are not sure of that can later be disproven will only further risk damaging your company's reputation.

4. Keep The Channels Of Communication Clear

Have a separate communication plan for employees, partners, clients and media. Be clear on how they can get in touch with you if they have more questions, and appoint a representative from your organization who will be the main point of contact for each channel. Make sure that person is properly prepared and trained with the appropriate communication response.

5. Offer Restoration Services

Depending on the ability of your organization to cover such costs, and depending on the type of breach, consider offering restoration services like identity theft protection services. Because stories of breaches happening in the news are so constant, many customers understand that a breach of their data could very well be inevitable. That being said, it doesn't make their experience any better. A sincere offer to help your clients overcome the breach of their data could go a long way in helping keep your clients' trust. Mistakes happen. How we go about fixing those mistakes is where brands are made.

When we think of preparing our organizations for cybersecurity, we often think of firewalls and antivirus solutions. But it's now time for us to expand our way of thinking from hardware and software to insurance, legal and PR. Cybersecurity is so much more than it used to be, and anything that can damage a company's brand to the point of no return needs a well-thought-out PR strategy.