BIZCOMMUNITY

How businesses can use PR (Public Relations) as part of their cyber security management

By Lerato Mpholo , issued by Opinion & Public BCW

22 Aug 2022

Cyber-attacks continue to rise in line with the proliferation of digitised business models and systems. Sophisticated attacks like data breaches, trojan horses, phishing, ransomware, and business email hijacking are typically left in the hands of Information Technology (IT) or cybersecurity divisions in many organisations. Though PR professionals may not play an active role in preventing cyber-attacks, they can contribute to the overall cyber security of an organisation.

Lerato Mpholo

The cost of an attack on a business is double-pronged: it is quantifiable and non-quantifiable. Quantifiable costs include paying fines, and overhauling IT infrastructure, while non-quantifiable costs include the loss of crucial business intelligence and a crippling blow to a business's reputation. As recently seen, large organisations like BET9ja in Nigeria, and TransUnion in South Africa battled cyber security breaches for extortion.

According to McAfee cybercrime cost the global economy USD $1tn in 2020, an amount which Cybersecurity Ventures expects to increase to USD $10.5tn by 2025. With such alarming figures, most businesses may find it strategic to involve the PR function in their cyber risk management approach. This is ideal before and after an attack, as much as it is during one.

PR practitioners who are the natural custodians of an organisation's information distribution, play an essential role in the management of non-quantifiable costs of cyber-attacks. Within an organisation, PR facilitates a lot of information with stakeholders.

Human life is more interconnected to the advanced technology we enjoy today, and devices carry a lot of confidential information. Therefore, it has become crucial for the PR department to educate the public about cyber security because it directly affects the business and by extension the personal lives of those associated with the business. PR can do the following to help manage cyber breaches:

- ***Understand how a cyber-attack can damage an organisation's reputation*** - The PR department handles keeping and growing the reputation of a business. A single cyber-attack can undo years of hard work put into constructing a business image. So, it is important to ensure that stakeholders clearly understand how even a small piece of information in the hands of hackers can irretrievably ruin a brand in the eyes of its various stakeholders.

- ***Drive education on the impact of attacks*** - The PR department understands potential reputational costs of cyber-attacks. Working with the information security officer, it can pass this knowledge on cyber security to the company at large. This can sensitise employees, suppliers, and others on attack methods, helping them to find and not click on links in unsolicited emails or messages as well as suspicious attachments can help in proactively minimising potential attacks.

- ***An integrated cybersecurity threat incidence checklist*** - This document would supply real-time updates on potential attacks. Developing this checklist requires a collaboration between the PR and IT department.

After a cyber-attack, the PR typically communicates the incident to an organisation's stakeholder groups. The immediate task after an attack is usually the activation of a crisis team to work with business functions such as legal and IT to ensure correct reporting. Communication after an attack is key to alleviating fears that a business might hide the severity of the attack. The following are also some post-attack actions that PR practitioners within an organisation can take:

- ***Reputation management through social media*** - Social media is a fast and powerful tool which PR can use to connect with customers and clients. Social media platforms can be used to notify and reassure stakeholders that a situation is under control.

- ***Create an incidence Frequently Asked Questions (FAQs)*** - When an attack occurs, internal and external parties have questions. These questions are centred around how an attack occurred, when it occurred, how it affects customers or clients as well as what the organisation is doing to prevent a recurrence of a similar attack. Instead of letting the media and other news entities control the narrative of an attack, PR can publish an FAQ (Frequently Asked Questions) that is updated regularly address all pressing questions about the attack.

- ***Publish organisation-wide incidence reporting guidelines*** - After an attack, internal members of an organisation might want to talk about the cyber-attack incident to reporters and clients or share information on social media. To control the narrative, PR may find it useful to create incidence and publish reporting guidelines which will ensure all the information about the attack comes from one source and such information is issued correctly.

- ***Conduct post incident analysis, evaluation, and reputation review*** - A cyber-attack will affect a business's standing. PR should analyse the severity of the incident, evaluate the impact, and review the business's reputation. The post incident analysis also entails the creation of a recovery plan to manage the reputational fallout, regaining confidence and rebuilding trust with key stakeholders.

PR should take great care when responding to cyber-security-related incidents during and after an attack. The IT department may be the vanguard against cyber-attacks but, PR has the effective means to communicate. This needs the partnering of IT and PR business functions in developing cybersecurity plans. A partnership of IT and PR enables both functions to create robust, credible, and resilient cyber security plans.

ABOUT THE AUTHOR

[[https://www.linkedin.com/in/leratokiviet/ Lerato Mpholo]] is a senior communications consultant at [[https://weareopinionandpublic.com/ Opinion & Public BCW]] and a member of PRCA Africa NextGen Group. She supports an array of multinationals in Francophone Africa delivering corporate communications. She has over a decade's experience in PR and, communications in South Africa, Kenya, Ghana, and Nigeria and has a key focus on technology.