STRATEGIC COMMUNICATIONS

Rebuilding Trust Following a Cyber Attack

Warren Buffett once said, "It takes 20 years to build a reputation and five minutes to ruin it." Rarely can the 'sage of Omaha' be disputed, but on his point around timing, five minutes is a very long time in today's real-time world when you're dealing with a cyberattack.

Cybersecurity is one of the most critical commercial and reputational risks facing South African organisations today. No sector is immune, and no business can afford to be unaware of their vulnerabilities or have robust practices in place to manage them.

This mounting risk, coupled with the always-on nature of news means that companies face round-the-clock scrutiny. Globalisation, investor activism, regulatory change, political and cyber risk are all contributing to increased business vulnerability which is amplifying the need for companies to carefully consider their ability to respond effectively.

Cyber risk is no longer just a technical issue, while both prevention and response need to be comprehensively embedded in people and systems. For it is how an organisation responds to an incident that is often as important as the incident itself.

The scale of the problem

The global move towards increased digitisation and cloud migration, combined with a regulatory and judicial environment that is pursuing greater effectiveness leaves us in an exposed position.

The fourth industrial revolution is fundamentally changing the risk environment and creates a new range of potential unintended consequences across corporate ecosystems. Unfortunately, Africa's pursuit to realise the potential of the fourth industrial revolution is not equal to its efforts in cybersecurity and this is leaving the continent vulnerable to cyberattacks.

Today, cyber threat tops most corporate agendas. Research conducted as part of FTI Consulting's Resilience Barometer amongst companies operating across the G20 countries at the beginning of 2019 found that the biggest threat to resilience is that of 'cyber-attacks stealing or compromising assets' and 30 percent of those companies surveyed said this had happened to them in 2018.

Yet whilst 28 percent of business leaders predicted this will occur to them over the course of 2019, just 45 percent said they are taking proactive steps to manage this risk. Nearly four out of ten companies are simply reacting to a cyber attack when

it occurs, while 12 percent of executives say that cyber risks are not managed at all. Remarkably, even when a company has suffered a cyberattack over the past 12 months, it is not significantly more likely to manage its cyber risk proactively. Just 46 percent say they will be proactive in the future.

Furthermore, according to the Allianz Risk Barometer 2019, cyber security was named the top concern among South African businesses. And our government is acting. The Cybercrimes and Cybersecurity Bill aims to consolidate existing legislation and implement more stringent laws to stop cyber criminals acting in the country without fear of reprisal.

Planning for the worst

Today's cyber threat landscape is ever-evolving, with increasingly advanced tactics. Moreover, cyberattacks are becoming more sophisticated and targeted, therefore a proactive approach is essential. While a cyber breach can be over in seconds, its aftermath lasts much longer.

Waiting until an incident occurs to determine a response is too late. Every second counts and lost time equals lost information, resources and reputation. How companies react to and communicate regarding their cyber security incidents is critical and there is only one chance to get it right.

Whilst companies cannot control whether they are the victim of a cyberattack, the cyber incident response they enact is. Proactivity is key, especially when it has the potential to both cripple organisations and permanently damage the reputation of a company.

Understanding the risk

Information is at the core of a good crisis response plan, starting long before a hack ever takes place. Companies need to understand their threat profile, prepare a response plan, understand their weak points and harden their defenses in order to enable strong cybersecurity. Having data governance in place as part of a crisis preparedness and scenario planning impacts the effectiveness of the response if indeed the worst happens.

By understanding and employing cyber threat intelligence, organisations can gain a strategic advantage over malicious actors. However, converting cyber threat information into actionable, contextual intelligence that supports enterprise security decisions is the challenge.

Taking proactive action

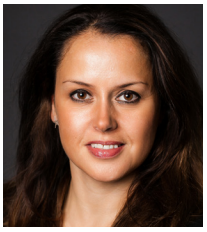
An integrated, cohesive strategy is key, implemented across existing mission critical functions. And it is this that informs both internal and external communications working from the inside out every step of the way. Addressing the various phases of an emerging crisis, reviewing options and making consequential decisions at each juncture.

Companies can mitigate the impact of the incident by stopping and recovering from it. Containment procedures can limit the scope and magnitude of the attack. This phase of incident response seeks to prevent data from leaving networks and prevent further damage. Eradication is the removal of malicious code, actor accounts, or unnecessary access, as well as repairing vulnerabilities that may be the root cause of the incident. Recovery is every organisation's top priority, but this can only begin once the incident is contained and eradicated.

But this isn't the end. One of the most important aspects of incident response is also the most often forgotten - learning from the event and improving processes. Organisations must evolve to reflect lessons learned, new threats and better technology.

The goal in the recovery process is to position the crisis as firmly in the past, emphasising the progress made to restore confidence and bridge to long-term sustainability. Once the initial crisis has subsided and recovery is underway, it is crucial to understand, identify and apply the lessons learned, facilitating continuous improvement and assured management of future issues.

Rebuilding trust damaged amongst clients and broader stakeholders is not a quick fix – it takes time to earn it back. A quick and effective response to a cyberattack is critical when it comes to limiting long-term damage.



Caroline Parker
Managing Director, Strategic Communications
caroline.parker@fticonsulting.com

FTI CONSULTING™

0825 - 10/19