Instinctif PARTNERS

Reputation Protection in a Cyber Attack

The frequency and sophistication of high-impact cyber attacks against companies is increasing at an alarming rate. A growing wave of ransomware attacks is affecting companies of all sizes from critical national infrastructure, product manufacturers, supply businesses, political parties, charities and SMEs.

Taking practical, technical steps is essential to reduce the likelihood of an attack, and preparing the processes, and critically, the communications you need to deploy in the immediate aftermath of a cyber attack will help protect your company's reputation and value.

> *We've seen twice as many attacks this year as last year in the UK.*
>
> GCHQ, October 2021

Ransomware is evolving – denial of access attacks now include threats to publish or sell data extracted from your business, risking significant embarrassment and financial loss. Alongside the damage of the attack itself, individual victims of any data breach such as personal or bank details, commercially sensitive data or copyright infringement could all result in a secondary level of loss for a business in fines or compensation.

Containing the impact on your business requires you to act quickly, taking immediate actions not only to protect your systems but to safeguard your hard-earned reputation and value .

Instinctif Partners can help

A cyber attack against your business could last a number of weeks, but the time pressures you will face will be immediate – especially if you're a listed business. How you engage with your stakeholders from day one will determine the impact on your reputation and the value of your business. We will help you be better prepared, buying you critical time in the early stages of your cyber attack response.

Perception matters. Research has shown that companies who respond well to a crisis go on to outperform investors' expectations by **20%**, whereas those who perform badly will underperform by **30%**.

Our integrated approach brings together decades of capital markets, corporate communications and specialist crisis expertise so your business is better prepared to respond to and recover from a cyber attack.

As a first step to response preparedness, we have created **CyberOptic,** a proprietary diagnostic tool which enables you to benchmark your organisation's current response plans against best practice.

Our services

Whether you need to create a full cyber response communications plan, to develop your stakeholder engagement activities or are seeking a review of your existing preparedness against best practice – we can tailor support and expertise to suit your tactical and strategic objectives. And if the worst does happen, we can support you to navigate through the challenges and protect your reputation.

For more information, to book a complimentary 30-minute consultation with our specialist risk and crisis team or to discuss how Instinctif Partners can help you, contact:

Email: riskandcrisisteam@instinctif.com

Practical and strategic support

- Senior strategic counsel for C-suite and Board
- Benchmark communications preparedness against international best practice
- Development of cyber crisis communications plan
- Cyber attack action planning and preparedness
- Tailored stakeholder mapping and prioritisation
- Cyber crisis communications materials for all stakeholders – investors, media, clients/ customers, employees, government
- Advice on market announcements and regulatory notification
- Co-opted support onto your crisis response team
- Training and embedding of enhanced cyber crisis prevention measures
- Scenario planning and simulation exercises to test your teams
- 24/7/365 on-call crisis retained support
- Provide an outsourced platform for all crisis management communications materials if your system is compromised or disabled
- Hosting your crisis management team calls
- Acting as the contact point for all media enquiries and handling engagement
- Setting up an emergency call centre for customer enquiries via our specialist partner
- Proactive engagement with government and regulators on best practice

> *A cyber incident impacted our business on a weekend and Instinctif responded immediately with comprehensive support and were on-call 24/7 throughout the 6-week critical time period as we dealt with the implications of the incident. Instinctif provided senior counsel and practical support that made a real difference and had our Executive and Board's full confidence. The partnership supported us in protecting our reputation with clients, investors, employees, and media, against what was a potentially devastating incident.'*
>
> **CMO, globally listed technology company**

Our experience

- Supporting a listed North American company throughout an aggressive ransomware attack in 2021
- Developing cyber crisis communication materials for a FTSE250 food and drink manufacturer in 2021
- Several months of crisis management for a German insurance company after a ransomware attack with data encryption, data theft and attempted extortion in 2021
- Simulation testing the cyber crisis plans of a global FTSE100 chemical manufacturing company
- Media relations and engagement for Zurich Cyber Risk Report published in collaboration with the international think tank, Atlantic Council
- Annual cyber-risk update for major insurer, including collateral, best practice scenario planning and scripting for intermediary roadshow
- Managed crisis communications, stakeholder and media relations for South African ISP during cyber-attack and customer account information data breach
- Managed stakeholder engagement, media relations and crisis communications for major, listed chemicals and explosives manufacturer during ransomware attack
- Supporting the UK's largest cybersecurity consultancy to shape UK trade policy for cybersecurity services
- Advising the UK Government's internal automation and cybersecurity think tank, Centre for Data Ethics and Innovation (CDEI)
- Securing radio spectrum access for UK energy infrastructure to increase their resilience and security significantly enhancing the hard cybersecurity of the UK's energy infrastructure
- Advising a cybersecurity innovator, GreyList, on how its automated fraud detection and investigation technologies could support UK Government Departments

For more information, to book a complimentary 30-minute consultation with our specialist risk and crisis team or to discuss how Instinctif Partners can help you, contact:

Email: riskandcrisisteam@instinctif.com