



Guide to Crisis Communications during a Cyberattack

COVID-19 is fast accelerating the digital transformation of business, including retail, education, financial, and healthcare. With this rapid digitisation also comes an increased risk and impact of cyberattacks on companies and individuals. Cyberattacks have been growing in recent weeks at an alarming rate, exploiting the unrest and social and economic situation created by **COVID-19**. Spikes in attacks also link to the **COVID-19** news cycle, suggesting attackers leverage breaking news to take advantage of vulnerable populations and business sectors. Corporate reputation and cyber risk go hand in hand and now more than ever, companies need to be prepared for a potential cyberattack with a solid crisis communications plan, protecting their business and brand.

Increased Threats of Cyber Breaches

The World Economic Forum (WEF) COVID-19 Risks Outlook found



particularly due to the shift in working from home practices. Cybercriminals are taking advantage of the COVID-19 pandemic by re-purposing their toolsets, deploying new infrastructure, and developing campaigns to proactively target frontline and vulnerable organizations. Global

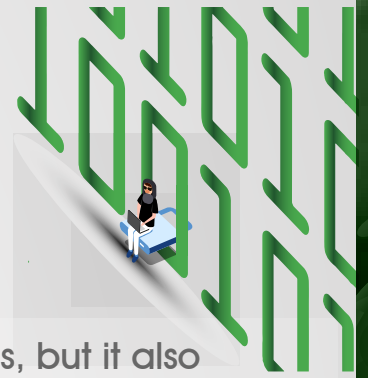


organizations have seen a 148% spike in ransomware attacks, with the finance and healthcare industry most heavily targeted.

Business decisions related to digital transformation in response to COVID-19 will add substantially to the rise of cybersecurity issues. Organizations need to consider how their new business models and remote working may have increased the risk of a cyberattack. Cyberthreats in the COVID-19 environment are only anticipated to increase over the course of 2020 and beyond. The global cost of ransomware alone is expected to reach \$20 billion by 2021. Malware has been used to exploit the fear of COVID-19, invading, or disabling computer systems and networks, with these attacks often performed through social engineering campaigns.

Cyberattacks Impact

Internally and Externally



Not only can a cyberattack affect critical business functions, but it also brings the added external pressure of attention from the media, the public, customers, and regulators. Companies must not have their ability to protect customers and employees questioned at any stage during a cyber crisis. Organizations must protect their corporate reputation as an increasing importance is being placed on business ethics and governance since **COVID-19**. Consumers, investors, partners, employees, and shareholders are holding organizations much more accountable for their actions.

A cyberattack itself does not need to destroy your corporate reputation; it is how you prepare for and handle such a crisis that will determine lasting trust in your brand. Managing the current increased cyber risk is crucial and means continually assessing your organization's cyber defences. Equally, it is vital to take steps to mitigate the impact on brand reputation with a solid crisis communications plan in place and a proactive communications approach.

Talk to Your

Audience

Dealing with a cyberattack on top of the **COVID-19** crisis is a major challenge for any organization to cope with and requires careful coordination between the incident response team and a range of internal and external stakeholders. Organizations should develop their crisis communications plan as a pre-emptive measure now and as part of their broader incident response plan with clear messaging and lines of communication to enable sound decision-making during the high-pressure environment surrounding a cyberattack.

This '**7 Steps** to Crisis Communications under a Cyberattack' Guide brings together **VIRTU**PORT's and **W7**WORLDWIDE's combined cybersecurity advisory and communications knowledge to create a timely tool for companies and organizations to help with their cyber resilience planning amid the ongoing challenges of **COVID-19**.

1 Review Crisis Communications Plan



Companies cannot wait for a breach or cyberattack to occur and must view their cybersecurity crisis communication plan in relation to **COVID-19** risk as an ongoing work in progress, updating it regularly with new potential threats as part of their incidence response strategy. A clear crisis communication plan will need the input and advice of the **CEO, CSO, COO, HR** and **Legal**. The response team needs to be able to give insight into all perspectives of a potential crisis and its impact on the organization.

The organization should determine the basics of who they will need to communicate with and what they are likely to be asked. Your cyberattack crisis communication plan should include details of your incidence team and their contact details, who will have responsibility for signing off key messages, a list of audiences and stakeholders you will need to reach and a list of channels that will be used to communicate your messages.

It is particularly important employees understand the increased danger of cyberattacks exploiting the **COVID-19** pandemic and part of the crisis communications plan should include an internal cybersecurity alertness campaign. Consider any mandatory obligation on your business to report cybersecurity incidents as part of your plan, especially in regulated industries such as banking and finance, and around data protection.

See **W7** WORLDWIDE's recently published Guide to formulating a comprehensive **COVID-19 Crisis Communications Plan** and ensure to keep hard copies of your plan in the event a cyberattack brings your entire systems down.

2 Crisis Simulation Practice



It is important to test your processes and systems to ensure your plan works and the crisis management team understand what is required of them should a cyberattack occur. Practicing your crisis response and robustness of systems will uncover crucial learning about vulnerabilities, communication priorities and gaps in your plan that may need to be addressed.

During **COVID-19**, many organizations hastily moved to working from home practices and new online business models, in the process often bypassing their existing cyber security procedures and policies which now need to be reviewed. Employees need to know how they report any concerns about suspicious activity, how to prevent the inadvertent spread of malware and the protocols in place to regularly update computers and protect passwords.

Develop blueprints for different types of cyberattack scenarios, testing how the crisis teams operate and coordinate with each other. This is even more important in an environment in which the incident response and crisis communications teams are operating remotely. Incorporate the operational impacts and pressure a cyberattack will put on your ability to service customers.

3 Control the Narrative



In the wake of a successful cyberattack or data breach, your organization needs to control the narrative surrounding the crisis. Ensure you are the first source to break the news to demonstrate transparency and trust between you and your stakeholders. Prepare to respond at the speed of Twitter and have dedicated communication channels ready to go. Carefully consider the timing of communicating externally, as your attackers may be warned, or the incident is overrated, and any damage was successfully contained.

Acknowledge there is a problem and that you are dealing with it. Release an initial Holding Statement to set out the facts you know so far, what your next steps are and key messages you want to convey. Communicate proactively, rather than retreating into denial or going on the defensive. Do not communicate issues that have not yet been confirmed as facts, adding fuel to speculation or conversation surrounding the cyberattack. Update your audiences at regular intervals to keep them informed of the latest information to remain in control of your message.

Implement a robust notification plan for your customers, employees, and other relevant stakeholders. Managing the communications around a cyberattack are just as important as managing the breach itself. The people involved in the notification process need to include IT and cybersecurity to analyse what happened. Legal counsel to advise on regulatory risks and to vet communications. Corporate Communications and the CEO to relay relevant information to the public.

4 Monitor Social Media



Social media is a critical and fast moving channel of communication between organizations and the public. Social media can provide the incident response team with valuable information and a read on customer sentiment. Stringent media monitoring at this time will help alert you when to initiate intervention before rumours start to get out of control. Social media reports can also provide the team with important indicators of service performance, information disclosures and other facts that might shape the response priorities.

Ensure there are clear social media guidelines for employees in place and monitor their activity as in some cases in-house whistle blowers leak information that leads to the cyber incident. Adapt your Holding Statement for social media in case of questions or comments. Create a framework for answering questions honestly and with integrity.

Rapid and effective communication via digital channels is an essential component of a strong response to cyberattacks. Solid crisis communication plans provide mechanisms for swiftly notifying stakeholders, coordinating internal and external stakeholders, and monitoring public reaction. These tools improve the organization's ability to respond and help to minimize reputational damage.

5 Key Spokesperson



When under a cyberattack, the press office and incident response team will be overwhelmed with inquiries and questions from customers, the media, regulators, and other stakeholders. Your crisis communication requires a co-ordinated response to prevent rumours and ensure consistent messages across all communication channels. Organizations should nominate a key spokesperson to take on the company spokesperson's role to provide a consistent view and voice of the incident to internal and external stakeholders.

The spokesperson needs to have specialist communications skills and be media trained, rather than requiring a deeply technical background. The technical team provide the necessary information to give the company spokesperson enough familiarity with technical concepts to serve as a translator for the technical information emerging from the response team. A glossary can help ensure the wording in written and verbal communications is used correctly and consistently.

Convey facts in a straightforward, conversational manner and have the company spokesperson speak on a regularly scheduled basis to stabilize contact with the press and the public. Use respectful jargon-free language and a serious tone that reassures target audiences of your commitment to dealing with and resolving the cyberattack. Communicate continuously and from the top, with direct input of the CEO, who may in fact also be the best nominated company spokesperson.

6 Target Your Messaging



Creating an effective Cyberattack Crisis Communications plan will include a stakeholder analysis to have a clear and complete understanding of who the organization needs to communicate with and what each audience's unique interests and needs are. Investors and shareholders will not have the same focus as employees, supply chain partners, customers, or government authorities. Customize your talking points to convey what is most important and top-of-mind to each audience, carefully plan how to reach each audience and who will speak to each one.

Your Cyberattack Crisis Communications Plan needs to anticipate that an incident will require communication with your customers and the public. This may be a mandatory notification of a data breach or an explanation to customers of service disruption. The cadence and content of these communications will have a significant impact on how your organization is perceived in how effectively and expeditiously it is handling the crisis.

Develop communication templates for customer outreach as an important tool in your crisis communication planning. These can be provided by the communications team to the incident responders to help craft mindful and approved notification messages. Pre-approved templates remove hurdles in advance, enabling the incident response team to fill in the blanks. Include statements that inspire confidence in the company and where possible commit to action, such as timelines for having the issue resolved. You need to follow through on the dialogue you started and keep your stakeholders and customers up to date on new security measures.

7 Moving on from a Cyberattack



The period following a cyberattack is not easy to manage for companies. Lots of time and effort will need to be spent in the aftermath to restore trust. Companies must continue proactive communication with their customers and stakeholders, outlining plans for preventing future attacks and remedial actions that have been taken.

Implement a post incident reform programme with education and technical upgrades to protect data, employees, and customers from future cyberattacks to rebuild brand equity. It is imperative to include this as part of your communication strategy, including the remedial steps taken to prevent a future incident, assuring the public that you are well prepared at all times.

Proactive planning, including a communications strategy, using narratives that resonate with your customers and the public will avoid prolonged brand damage and loss of public trust. Follow-up conversations around the event with new knowledge and learning that may help other businesses or organizations. Make a positive contribution by engaging in threat sharing initiatives where companies share information about their cyberattacks to learn about evolving threats. This will ultimately help everyone with better prevention of the growing number of cyber threats and position you as part of the solution to the problem. Take the leadership position in your industry to educate on the topic of cybersecurity in **COVID-19**.



Consumers are sceptical that organizations can handle their sensitive information and are now more than ever paying attention to what is happening with their data. The impact of a cyberattack on brand reputation and shareholder value can be substantial following an attack. Stakeholder opinions about how well a company managed an attack is critical to business resilience and recovery from the crisis. A favourable corporate reputation plays a vital role in retaining customers, attracting the best talent, suppliers, and investment.

Fact-finding in cyberattack investigations takes time and whilst communications needs to move quickly, the Cyberattack Crisis Communications strategy needs to address how to deal with inquiries from stakeholders during the period needed to establish a factual foundation. This is to avoid the spread of misinformation or loss of credibility from saying something that has not been verified yet. During a cyberattack the communications team will be overrun to provide information as to exactly what happened and should be said and when. Having the processes of this set out in a Cyberattack Communications Plan prior to a breach ensures information is disseminated as quickly and accurately as possible.

Moving Forward



Organizations today cannot afford to think cyberattacks will not happen to them. They are inevitable and a liability and reputational risk to the organization. Crisis preparedness is the defining factor in how well your company can weather such a crisis. Cyberattacks can be complex, far reaching and debilitating on your business operations. A Crisis Communications and integrated incident response plan will provide a solid foundation to safeguard your business and reputation. This requires consolidating technical and legal communication with tactical corporate communication into a joint approach and concept.

✔ **IRTUPOINT** is a leading provider of cybersecurity services in the MENA region across all verticals, helping clients protect themselves from the growing number of cyber threats. **W7WORLDWIDE**'s experienced Corporate Communications team is currently working with both local and international clients to help them put their **Covid-19** Cyberattack Crisis Communications plans and strategies in place.

About **W7** WORLDWIDE



W7 WORLDWIDE is an independent communications consultancy based in Saudi Arabia. Our understanding of the local market converged with our global reach and knowledge enables us to bridge our clients with their audiences effectively. We are aligned by the objective of filling the gap in communication that exists in the local market. Therefore, our specialty lies in building bridges that sustain relationships and create brand reputation and value through innovative approaches. Our array of services includes, but is not limited to:

- Corporate Communications Strategy
- Stakeholder Mapping
- Crisis Management
- Corporate Social Responsibility
- Internal Communications
- Reputation Management
- Media Relations
- Public Relations
- Public Affairs
- Social Media
- Marketing & Brand Solutions

Notice: Proprietary and Confidential

All the content of this document (text, figures, list, financial information, graphics, designs, diagrams, as well as other graphic elements and/or audio and videos), whichever the format used (paper or electronic), is confidential and proprietary to **W7** Worldwide . This document includes ideas and information based on the experience, know-how, intellectual/creative effort of **W7** Worldwide .

For these reasons, this material shall not be used, reproduced, copied, disclosed, transmitted, transformed, commercialized, or communicated, in whole or in part, neither to third parties nor to the public, without the express and written consent of **W7** Worldwide .

W7 Worldwide © All rights reserved

For more information:

Our Official Website: <http://www.w7worldwide.com/>

 +966 12 661 4579

 +966 56 720 1039

 info@w7worldwide.com

 www.w7worldwide.com

 @w7worldwide