AlixPartners

MARCH 2020

COVID-19 RESPONSE

ESSENTIAL STRATEGIES FOR MANAGING CYBER RISK IN DISRUPTIVE TIMES

Five key tactics for business leaders to minimize risk in a dispersed, high-velocity environment

As COVID-19 continues to dominate headlines around the world, organizations have moved decisively to protect their staff and customers through travel bans, office closures, and remote working arrangements. Typical business continuity plans are based on denial of access scenarios to specific buildings and physical facilities–but, in the face of a pandemic, where do you go?

The outbreak of SARS in 2002/3, and the subsequent focus on flu pandemics, has led more companies, across all industry sectors, to consider how they would increase resilience in the face of extreme numbers of staff not being contactable or available to work. But do these plans reflect current business realities, such as updated organizational structures, evolutions in technology, or necessary increases in reliance on third parties?

What is the impact of a dispersed workforce on your business?

Homeworking, social distancing, and self-quarantine may help to mitigate the risk of a virus taking hold within a workforce, but each introduces practical challenges and raises questions and risks of its own. Concurrent demand on remote access solutions will impact capacity in terms of bandwidth, licenses, and hardware. There is also a risk that as capacity is stretched, mistakes will happen, or corners will be cut.

In such an environment, it is easy to imagine that information security may be forgotten.

Increased home working also expands the attack surface for cyber criminals, who will leverage the disruption caused by targeting companies at vulnerable points, such as payments. Given the volume of media attention, threat actors are already running virus-related phishing campaigns. The World Health Organization has issued a warning that criminals are posing as officials to plant malware to disrupt business operations or elicit funds.

Strategies and tactics to navigate the current remote working landscape

1. DON'T IGNORE THE CRITICAL BUSINESS-AS-USUAL SECURITY TASKS

In times of crisis, it is easy to forget or ignore everyday business risks. Ensure you have validated, current backups that are performed in line with policy. Be confident that your recovery processes and tools are also current and fit for purpose, with multiple people having the physical (keys) and logical (user profiles/permissions) access to recover business-critical data.

To enable mass remote working, many decisions may be made for expediency without consideration of risk. Continue to deploy operating system patches and anti-malware. Don't forget your adversaries are looking for holes and a way to exploit weaknesses, especially during a crisis. Continue to perform systemic monitoring of network traffic flows and reviews of key system logs to mitigate the risk of compromise.

2. MAINTAIN CLARITY ON HOW YOU WOULD RESPOND TO AN INCIDENT DURING THE PANDEMIC

While minor in comparison to the pandemic in which we are currently engulfed, normal incidents will occur. Systems will go down, hardware will fail, and the bad guys will continue to try to disrupt your business, steal your data, or simply embarrass you. Typically, firms have incident processes in place, so don't ignore what has already been done: leverage the tools and capabilities available to you.

If not already operating a split-shift pattern, think about segmenting your teams, so that there is capacity and capability to respond to an incident.

Consider how you'd manage third-parties in an incident management scenario. Services you rely on might not be immediately available.

3. KNOW YOUR "RED LINES", BE CLEAR ON MINIMUM CONTROL STANDARDS, AND CONSIDER RISK APPETITE

Have clarity on the red lines or non-negotiable control standards. This may mean temporarily adjusting risk appetite, but be aware that with a reduced workforce, impact tolerances may also be reduced. If changes to processes and protocols are needed for operational reasons, it is essential that cyber risk is a key consideration. However, the risks associated with this decision need to be clear and a plan should be in place to revert to normal operations once the crisis is over.

Continue to operate governance processes to effectively manage non-incident related risks and issues. It is important to remember that, often, temporary things become permanent. Do not allow the value of your business to be compromised through a data breach caused by consciously accepting a risk too far.

4. ESTABLISH A SUSTAINABLE OPERATING TEMPO THAT CAN BE MAINTAINED THROUGHOUT THE CRISIS

COVID-19 will be here for a while. Nothing in recent memory has been as global, nor as enduring, as this pandemic. Your teams cannot sustain crisis mode for months on end. What does the new business as usual look like for the next 6, 9, 12, or 18 months? Urgency and expediency are key characteristics of a response to crisis, but how many firms can continue to hold multiple war room calls a day?

Leadership needs to lead and demonstrate by example, maintaining a work-life balance for the wellbeing of your people. Be conscious of key people creating work during troughs in the operating rhythm, when they would be better off resting and recuperating. When facing a prolonged siege, your team must be ready to face challenges tomorrow and the day after, as well as today.

5. PREPARE FOR RECOVERY AND BUSINESS AS USUAL

There is no doubt that the COVID-19 pandemic is going to change the way we work. Make sure lessons are learned and applied to contingency plans–and not kicked into the long grass. Ensure post-mortems reach across and through the business. This will happen again, so seek a best-of-breed response, proportionate for your business. As firms return to pre-pandemic operations, restoration of non-essential services needs to happen in a systematic and structured way.

Consider performing penetration testing against your perimeter, and scan critical infrastructure components for vulnerabilities. In high-risk environments, assume a compromise has occurred and actively seek evidence of threat actors being live on your network. Have clarity on revised contingency plans and make time for robust scenario testing to prove resilience.

AlixPartners

For more information, get in touch: www.alixpartners.com/contact-us

ABOUT US

For nearly forty years, AlixPartners has helped businesses around the world respond quickly and decisively to their most critical challenges–circumstances as diverse as urgent performance improvement, accelerated transformation, complex restructuring and risk mitigation.

These are the moments when everything is on the line–a sudden shift in the market, an unexpected performance decline, a time-sensitive deal, a fork-in-the-road decision. But it's not what we do that makes a difference, it's how we do it.

Tackling situations when time is of the essence is part of our DNA–so we adopt an action-oriented approach at all times. We work in small, highly qualified teams with specific industry and functional expertise, and we operate at pace, moving quickly from analysis to implementation. We stand shoulder to shoulder with our clients until the job is done, and only measure our success in terms of the results we deliver.

Our approach enables us to help our clients confront and overcome truly future-defining challenges. We partner with you to make the right decisions and take the right actions. And we are right by your side. When it really matters.