The COVID-19 Corona Virus: Sustaining IT Operations In a Crisis

IT and information security leaders should consider three questions to assess the potential impact to people, facilities, and operations within their organization.

Right now, the world is watching to see how the coronavirus (COVID-19) spreads and how governments react to prevent and respond to infections. We don't know how much more the disease will impact normal day-to-day, but it has already inflicted material consequences on travel and several other factors that are important to IT managers and technologists.

With COVID-19 recognized as a pandemic, it's time for every information technology group in the world to look at key "what if" questions—what if COVID-19 (or something like it) directly impact regions where our people or facilities are located? How will governments respond, and how will that response impact our IT operations?

Depending on your industry, your management may have the expectation that you will continue to support the business as usual. While they may have that expectation, you may or may not be ready to fulfill it.

Thinking about this problem in advance is vital. Hackers understand the problem and see this as an opportunity to compromise public and private sector organizations who are not able to maintain their usual level of security.

For example, one frequent recommendation in epidemic/pandemic conditions is to have workers stay home and, if they can, work from home. For many businesses this is possible—at least in part. For others, where having workers at an office, store, warehouse or other specific location is a requirement, working from home may be impractical or impossible.

Regardless of that, every IT manager must focus on the question of how their organization is going to function. Consider these questions as a starting point:

Can our people work from home?

- If your system isn't built to allow remote access, and if you haven't arranged for a secure way to handle remote access to potentially sensitive and valuable information, you have a problem.
- If you're going to use a mobile data management system, it must be configured and ready to use.
- If people are going to need devices (laptops or tablet machines, for example) the organization must be ready to supply them.
- If people who need to work from home don't have home-based internet access (with sufficient bandwidth for your/their needs), they won't be able to do their job.
- If you need to develop more granular access controls in connection with remote access, it must also be ready to go. Assume that things will go wrong. Remote IT personnel may have to share duties or handle tasks that others who are unavailable can't handle.
- Check with your legal counsel: is there anything about the work at home environment that would require people to sign additional agreements to protect the organization? If so, you need to put those agreements in place.
- How will you handle help desk calls? If your people aren't going to be in the call center, can your telecon system distribute calls to alternative numbers (employees' home land-lines or cellular phones?) Remember that your call center or help desk may be

supporting people who live outside of the zones affected by the virus. Those people may not even know where in the world your help desk/call center is.

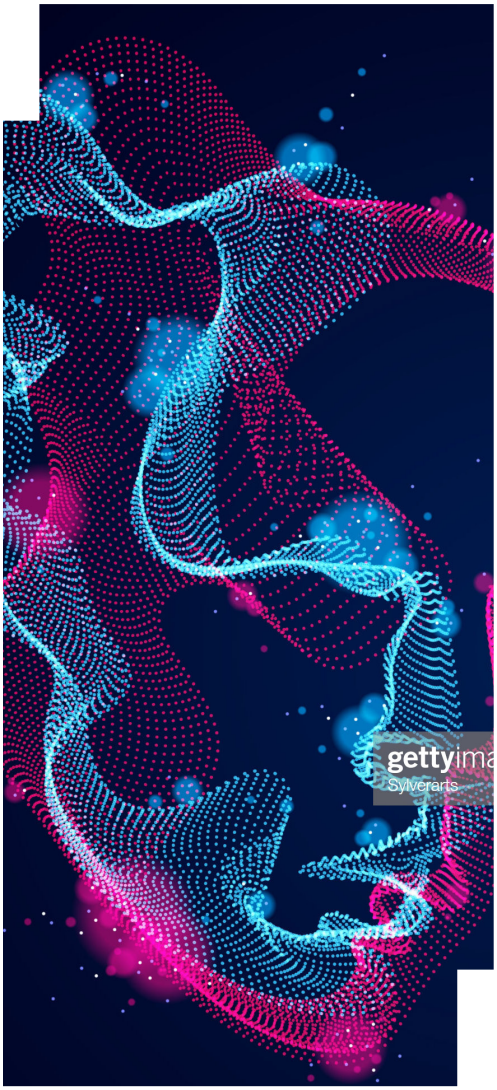
Do you really know if you're ready?

- Have you tested the alternative work remote environment under real world conditions? Without testing, you're betting a lot on your solution working and scaling as it needs to. Processes that work spectacularly well in a test environment may not scale as expected.
- Work through problematic what-ifs. What if cellular networks become overloaded? How can you communicate with remote employees? Do you have the tools to rapidly communicate with your entire team if they are working in a dispersed environment? Or to know who is or is not able to continue working remotely?
- Are your vendors and outsourcing partners ready to support dispersed operations? Do they have pandemic plans and have they tested them through exercises?

Can you maintain cyber security under exceptional conditions?

- What if travel to and from your security operations center (SOC) is restricted? Can your SOC operate remotely with the SOC team working from home? Are the SOC's systems ready for that form of operation?
- How will you deal with incidents and potential incidents? You should assume that you will likely have to deal with all issues with a more-or-less remote response. That could be difficult if you aren't prepared for it and haven't had a chance to practice working in that way. If you can, take the time to do a simulation of running the SOC in a lights-off remote personnel situation.
- If you're dependent on third parties for security, find out how they are prepared to deal with the challenges of a pandemic. They could turn out to be your weak link!

Even the best preparations may not be enough, depending on local conditions. But what is certain is that IT organizations that take the time now to plan for remote pandemic operations will be in a better position to respond—and to provide a true picture of capabilities to management—than those who sit back and use a "management by hoping for the best" approach.



AUTHORS

Alan Brill
Senior Managing Director
Cyber Risk, Kroll

Stacy Scott
Managing Director
Cyber Risk, Kroll

TALK TO A KROLL EXPERT TODAY

North America	UK	Australia	Hong Kong	Singapore	Or via email:
T: 877.300.6816	T: 08081012168	T: 1800870399	T: 800908015	T: 8001013633	CyberResponse@kroll.com

About Kroll Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security and data and information management services. For more information, visit www.kroll.com.

Duff & Phelps is the global advisor that protects, restores and maximizes value for clients in the areas of valuation, corporate finance, disputes and investigations, cyber security, claims administration and regulatory issues. We work with clients across diverse sectors on matters of good governance and transparency. With Kroll, the leading global provider of risk solutions, and Prime Clerk, the leader in complex business services and claims administration, our firm has nearly 4,000 professionals in 25 countries around the world. For more information, visit www.duffandphelps.com.