cybereason

GUIDE:

HOW TO MAINTAIN SECURE BUSINESS CONTINUITY WITH A REMOTE WORKFORCE_

Secure Your Organization Outside the IT Perimeter

BUSINESSES AROUND THE WORLD are experiencing a tremendous evolution as they take steps to protect their employees. We are experiencing this change ourselves, as we have moved our global security operations center off site to keep our team and the community safe. Thanks to years of experience and leading technology, our team is prepared to work from anywhere. However, we recognize that not every team is so robustly outfitted.

As attackers take advantage of the ongoing crisis, this becomes more important than ever. We are here to help across all corporate functions, and to provide professional services to help those struggling to adapt to the rapid changes triggered by COVID-19. Below, you will find perspectives from several of our experts with experience from managing crises across security and business functions.

As always, if you have any questions or need any assistance during this difficult time, reach out to us and we will be in touch as soon as possible.

THE REALITY OF THE IT PERIMETER

Thoughts from Sam Curry, CSO, Cybereason

FOR YEARS WE'VE HEARD in information security that "the perimeter is dead," but now is the time that we test it. The IT perimeter definitely exists; we can point to firewalls and DMZs and a loose correlation in most companies between some types of digital assets and the physical boundaries of the company. But the notion that the perimeter can stop serious, advanced attacks has long been put to rest. The real test now is if the business can survive outside of the perimeter, immediately, and if so, how to secure it.

Older companies in particular have some functions in G&A, operations, manufacturing and other key functions that are still very much tied to physical locations and to older IT stacks that even when IP-enabled are still only allowed local access and interaction. ERP systems and some mainframe applications are good examples of this; it's not that they can't be enabled for remote access but rather that many have not been allowed access from beyond the perimeter. There are three simultaneous problems to solve for any business faced with frightened employees or with customers and partners who don't want to meet face-to-face.

The three simultaneous problems to solve for:

01. **How do you navigate policies surrounding the current crisis?**
02. **How do you maintain as many business functions as possible when no one comes to the office?**
03. **How do you secure the enterprise when the office becomes only a mailing address?**

Let's look at these one-by-one, but first keep in mind that you don't have to remove all risk. The golden rule is that **companies exist to take acceptable risk for acceptable return on behalf of their shareholders**; but we'll come back to that at the end.

HOW DO YOU NAVIGATE POLICIES SURROUNDING THE CURRENT CRISIS?

First, the "policies on the current crisis" problem, which can be extended to policies around any pandemic or worldwide crisis. As executives of any stripe, it's important to be aware of how dangerous the threat really is or isn't and to dedicate people to understanding the data and the facts as they change. Most importantly, know that the data will inevitably be lagging real-time, hard to verify and subject to change.

This brings us to memespace and specifically to the idea of the crisis in the popular mind and imagination. Make no mistake, this is a very real and potentially very dangerous space; the memespace is as real as any physical space. In addition to tracking the data, business executives and security professionals should also track the discussion and information about the crisis. The idea of the crisis will have a life of its own, and will only loosely correlate to the data that you're tracking from the first exercise. Do not dismiss fears or emergent behavior as irrational because they don't track the data but rather deal with the ideas as fully real and deserving care and attention. If your employees are afraid to come to work, that's real and needs to be respected and addressed. If your customers and partners don't want to shake your hand or new protocols emerge around interpersonal interactions, that is likewise very real and will require thoughtful consideration and policy making.

HOW DO YOU MAINTAIN AS MANY BUSINESS FUNCTIONS AS POSSIBLE WHEN NO ONE COMES TO THE OFFICE?

Next, the "maintaining business functions" problem. At some point, whether in the current X-demic ("X" is used here since calling it an epidemic or a pandemic seems to be political and a subject of debate) or at some future point when the next X-demic arrives, companies will have to look function-by-function and as a whole at the need free themselves of all perimeters and still maintain operations, perform transactions and manage risks. Now is the time for some to decide who gets to stay home and who doesn't or, perhaps, to get ready for such a time. If you're in an unaffected geography, do the homework now. If you're in the thick of it, it's decision time; and now is the time for IT to shine.

For some this is an easy transition, especially smaller and newer companies that are already more-or-less remote businesses. For most, some functions are already remote, like sales or field marketing; but be careful because the nature of activities, travel, expenses, processes and the like will change. Your sales people may not be in the office since they are in other people's offices, but that doesn't mean they are ready to keep performing when told to stay at home. And of course there are some more traditional businesses that aren't ready at all for being cut off from physical buildings like factories, headquarters and customer-serving premises in hospitality, retail or transportation to name a few. Perhaps the most important thing to do is to ensure that HR and IT continuity support are if anything overly generous at this point in time: if people feel isolated, feel unsafe or can't get support they may panic and suffer needlessly.

HOW DO YOU SECURE THE ENTERPRISE WHEN THE OFFICE BECOMES ONLY A MAILING ADDRESS?

All of this brings us to the "securing the enterprise when no one comes to the office" problem. And this is hard to generalize since there are so many types of business. However, here's a list of the basic things to consider; but don't just read and panic. Rather, read this list and make some notes in an unordered list. This will form the first step of a plan because you can't do it all and you shouldn't try. Your job as an executive, security or otherwise, is not to eliminate all risk but rather to reduce risk in an optimal manner.

↘ IDENTITY

Is your source of corporate identity accessible to the outside? Do you use strong authentication in all cases, and if you suddenly switch it on, will people be able to assert their identity in a strong manner and allow them to authorize and exercise entitlements? In layman's terms, will they be able to claim their identity in a way that you trust and do the things they are supposed to do?

↘ REMOTE ACCESS

You might have some employees remote right now, but are all of them remote? Do you allow insider information to be accessed from remote, source code or strategic project documents like M&A named projects? Obviously, the VPN and your extranet strategy here matter and burst licensing might be required from suppliers, but consider by department what new data types are being accessed and what this exposure might mean from a risk perspective.

↘ ENDPOINT SECURITY

This is more than just hygiene and checkmarks, as are common with EPP solutions: DLP, Antivirus, Personal Firewalls, etc. While these are important, the endpoint is about to become for many the newest, most distributed place where your corporate data exists.

- **MOBILE:** Amazingly, this might be the simplest on the surface of all endpoints because many companies already allow personal phones or have a BYOD policy. However, even before going remote, mobile is still a vulnerable medium and needs better security measures generally. Now might not be the time to beef up mobile, but the day is coming post-crisis when that is likely to be the hottest risk area for many businesses.

» **LAPTOPS & DESKTOPS:** In a very real way, every employee will be working on data that is by definition outside the perimeter. If you don't already use tools like Full-Disk Encryption, now is not the time to turn it on blindly but rather to take note of what data is most sensitive and to come up with a policy for data-at-rest outside the company.

Security Operations and IR: security operations and incident response are often group activities with highly specialized collaboration and tool use. Can your employees exchange ideas, talk, meet ad hoc, exchange data and so on securely? It might be time now to send a few home and make sure that the work can still be done before everyone potentially heads home for a few weeks.

↘ PHYSICAL SECURITY

This might be one of the biggest areas of concern. When your employees take the machine home, what is their home work environment like? With other family members present and perhaps connecting on live social media streams, bringing other devices nearby or even the security of facilities, do you have simple policies that real human beings can follow to protect keyboard access, employee safety and media security? Do you have policies for what employees should do if they have a home break-in, if they suspect someone is eavesdropping on them in their personal space or if they feel unsafe working in their home environment? **Remember, not all employees have a home and personal space outside the office like yours.**

↘ AWARENESS TRAINING

It might be a good time to encourage a refresher in awareness programs and training as people move home. It will give them something to do and make them actively conscious of security issues. I suspect that there will be a few new modules in most awareness curricula soon around working from remote or at least an emphasis on these, but you can always encourage the creation of a new module around your company's move.

Let's return to the unordered list you are probably keeping now on a piece of paper, in a text document or in your head and to the notion that **companies exist to take acceptable risk for acceptable return on behalf of their shareholders.** This might seem self-evident, but executives who are contemplating closing premises during a crisis or planning for a future ability to do so should start with conversations at senior management levels right now:

01. Are you tracking the data on the current crisis and the real, direct risks to employees, customers and the business?

02. Are you also tracking the memespace and the very real potential risks and pains from media coverage, traditional or social media?

03. Which functions have to leave the building having never done so before? Can they do so and, if not, what has to be done to enable that?

04. Is there a critical function or bottleneck that would hamstring the business that you can identify right now?

05. Have you established a help desk or support function for HR and for IT continuity support?

06. From a security perspective, what new risks emerge due to Identity, Remote Access, Endpoint Security, Security Operations and IR and Physical Security? Can you rank order them and work on the most critical ones first?

07. If the business decides to turn out the lights in HQ today, can you articulate the new risks to be signed off on that will exist and the time-to-correction?

Finally, realize that attackers may use the crisis for phishing attacks, to find gaps in security operations, to target your employee homes and systems and may even create deep fakes in very targeted ways. Above all, communicate early and often with your employees.

REMOTE IS THE NEW NORMAL

Thoughts from Yonatan Striem-Amit, CTO, Cybereason

Companies looking to transition quickly from office-bound work to distributed remote work need to ask themselves three main questions:

01. **What are the processes and technologies to drive effective work without physical contact?**
02. **What are the core principles to enable productivity when working remotely?**
03. **How can you maintain business continuity and security when most or all of the workforce is remote?**

LET'S ADDRESS THESE ISSUES ONE BY ONE

WHAT ARE THE PROCESSES & TECHNOLOGIES TO ENABLE EFFECTIVE WORK WITHOUT PHYSICAL CONTACT?

For many workers, productivity depends on two key tenants: the ability to communicate effectively with peers, partners and customers, and the ability to access important resources and systems.

On the communications side, we've seen incredible progress over the last few years in technologies for teleconferencing. Zoom, Cisco, Google and Microsoft offer very cost-effective, cloud-driven tools that drive effective communications with multi-party meetings, a constant video feed, a shared screen and even a shared white-board.

In addition to effective communication, employees need access to resources like computer systems, files and data. Some organizations, especially those that are more established, may have systems on premise, whether it be payroll, production, or back office systems that need to be accessed on a day-to-day basis. To address this, organizations use Virtual Private Networks (VPNs), established technology that allows a business to temporarily extend their network to employee computers, laptops and phones, even when they are not present on site. This is a very effective tool for remote work, however, most companies have not planned for a scenario where a large portion of the work force attempts to connect to the VPN to access many internal systems at once.

For most businesses that allow remote work under normal conditions, only a small portion of the employee base will be working remotely at one time - say 5%. When an incident that forces social distancing occurs, in a matter of days, 100% of the workforce must transition to remote work.

This new reality requires careful analysis of capacity and prioritization of workloads: how much bandwidth will be available to each employee, what will access control look like, etc. It's important to bear in mind that not all functions are equal when it comes to service assurance.

This includes functions like IT: being able to consistently and effectively support the entire remote team is priority #1. Building in failsafes that can help diagnose what's going wrong is crucial. As an example, it can be a good idea to have a secondary dedicated VPN for IT personnel to support, should primary channels fail. Enable IT to log in remotely and identify how things have gone wrong, so the entire team isn't left stranded.

I encourage the readers of this article, first and foremost, to analyze their load capacity, licensing limitations, understand their ability to support their team, and increase available hardware and software to the point where IT is confident they can handle all employees working concurrently on the system.

Instituting a trial run before the actual worst case scenario hits is key. The first time an organization tries a 100% remote work scenario, they will most likely fail. They will inevitably discover previously unknown bottlenecks, which is why the trial is so important. Take a day for everyone to work from home before it is mandated by a crisis.

The main takeaway here: plan for the worst and hope for the best. Having a plan that has been tested will help the team understand and rollout deployment easier, and can make a huge difference in the future. Roll out deployment as much as possible before employees can't work and IT can't support them.

WHAT ARE THE CORE PRINCIPLES TO ENABLE PRODUCTIVITY WHEN WORKING REMOTELY?

While many companies have adopted off-site work for a small fraction of their employees and functions, transitioning to large scale remote work is very challenging not only from a process perspective but also culturally. Some employees require access to systems that only exist on premises, while others gain valuable satisfaction and fulfillment from face-to-face communications with peers, partners and of course customers.

Companies that have adopted the cloud early will discover that a large majority of their systems are already not bound to their physical office, while others, especially more established firms, are likely to rely substantially on tools deployed on premises or in their own data center.

Similarly, companies that have allowed some level of remote work will find their employees more experienced and quicker to transition to a 100% remote atmosphere. Employees used to working from home once a week will most likely have a better at-home work setup and understand the pitfalls of remote work already, which makes the transition easier than for those with no experience.

However, being mindful of the ways companies can facilitate remote work can dramatically help productivity. For example, instilling a culture of turning on video for a work call can help the team feel some level of camaraderie and social interaction.

This also brings up a challenging aspect for IT, especially when it comes to bring-your-own devices. With mandatory remote work, the majority of employees are of course unable to get into the office. The only bridge to work is through their laptop, or in some cases through their mobile device. The question is, how does this affect the help desk? How does this affect network control? Many organizations have built their monitoring capabilities based on the network. The problem is, now that employees are remote, monitoring the network will look like a connection to a single device. The VPN holds the entire communication, which makes it very difficult to identify various activities from a network perspective.

To address this, some organizations have mobile device management in place. Even so, at a constant distance, security becomes far less efficient and far more difficult. It puts a significant amount of anxiety on the heads of IT and security. The security topology for networks was about the separation of the inside and the outside by the IT perimeter. With all employees working remotely, our enterprise network now includes assets that are completely unmanaged, like every single employee's home assets.

HOW DO YOU MAINTAIN BUSINESS CONTINUITY AND SECURITY WHEN MOST OR ALL OF THE WORKFORCE IS REMOTE?

Transitioning to 100% remote also affects the agility of the IT and security departments. Unfortunately, hackers often take advantage of global incidents to find new ways to attack. But now, defending against these attacks becomes more complex. No longer can an employee with laptop issues hand their laptop to IT and get a loaner. Realistically, IT may not even be able to ship a laptop to an employee in a reasonable timeframe.

Further, there are a lot of risks around enabling rapid support requests. Prioritization must come into play, and first and foremost, baseline operation needs to be successful. Every organization should maintain a local stock of computers that are configured and can easily be shipped to an employee in the event of an incident. The best way to approach this is to simultaneously implement strong computer hygiene to ensure users don't install malicious software or take unnecessarily risky actions. Use a monitoring solution that monitors from the endpoint, instead of the network, like an endpoint security solution. Endpoint security solutions give visibility into malicious actions on the machine itself, remotely or on site, not limited to the network activity. Reducing risk comes from implementing a combination of security measures.

CLOSING THOUGHTS

The reality of remote work brings a lot of challenges to organizations, both process-wise and culture-wise. It is time for IT to show that the business can modernize itself very quickly to a changing environment when necessary. Doing all of that securely brings on its own set of challenges.

For many organizations, there is still time to prepare. Innovation should be starting now, by developing secure business continuity plans and simulating work from home scenarios to see exactly what works and what doesn't.

PANIC, SECURITY, & YOU

Thoughts from Amit Serper, VP of Security Strategy
& Principal Researcher, Cybereason

AS MORE AND MORE BUSINESSES move to remote work, it's important to take a step back and look at your business infrastructure to make sure that your business is doing the right thing. When sending people to work remotely, it's important to position your team effectively so you can add preventative measures against hackers.

In order to keep things simple and straightforward, let's look at this challenge in the form of a checklist:

↘ RECOMMENDATION 1: VPN

Many organizations are providing their employees with VPN access to the company's internal network. While IT staff usually maintain the network and keep it secured and patched, people oftentimes neglect VPN servers/appliances. We have all seen this happening fairly recently with multiple vulnerabilities discovered in the summer of 2019 in PulseSecure VPN and other products.

Giving your employees VPN access to the organization can help maintain business continuity, but can also be disastrous if they are misconfigured or unpatched. Please make sure that your VPN configurations, policies, and software/hardware are properly configured. Implement strong identify verification and authentication techniques and enable 2FA. You wouldn't leave your business' doors wide open and let anyone in, right? VPNs are the same.

↘ RECOMMENDATION 2: RAISE AWARENESS

Attackers will always release malware campaigns that exploit worldwide incidents. Remind your team that there are plenty of official websites to get any necessary information without having to download any "software." Also, make sure your employees can tell which emails are officially sent from company management. Attackers will try to exploit this lack of certainty to their favor with phishing campaigns.

↘ RECOMMENDATION 3: PHYSICAL SECURITY

While your cybersecurity may be up to par, make sure your physical security is too. If the office will be vacant for an unspecified period of time, no confidential information should be left on desks or out in the open. Secure rooms and safes must be properly secured and locked. If you have security cameras, make sure that they are online and properly configured.

↘ RECOMMENDATION 4: BE READY TO RESPOND

It's important to double and triple check that all of your backups are in place and that your company has a rapid response program that will allow you to recover quickly in the case of a ransomware attack. Having people working remotely can pose an extra challenge with this, which is why it is important to make sure that every security-doer in your organization, from your IT team to your security analysts to your incident responders, are ready and willing to take on the challenge if it does indeed arise.

↘ MOST IMPORTANT RECOMMENDATION: DON'T PANIC

This is perhaps the most important advice I can give.. If you decide that your organization is switching to remote work, go over the checklist rationally and slowly. Make sure that all of your security systems (physical and electronic) are properly configured, VPNs are patched, passwords are secured and rotated.

Spending an extra few hours or even a day going through these processes can save a lot of valuable time and money in the long run. While times of crisis are strange, stressful and new to us, technology allows us to overcome the challenges and fears that we have, as long as we remain calm and apply a good amount of thought.

CYBEREASON REMOTE WORKFORCE PROTECTION

Shai Horovitz, CRO, Cybereason

OVER THE PAST FEW WEEKS, we have been heads down thinking about how we can help enterprises through this new reality. During this difficult time, the remote workforce is exponentially increasing as both new corporate devices, home systems, and mobile devices gain access to enterprises.

Trying to simultaneously maintain business continuity while also defending a totally remote workforce is a complex issue with heightened risks. IT and security teams need support now more than ever, as teams struggle with balancing cooperative remote work and meeting the needs of an entire organization.

We are hearing from the market that they need to defend this new workforce but don't have the tools to do it. Because of this, we launched Cybereason Remote Workforce Protection. Cybereason Remote Workforce Protection is built to help organizations like yours secure this new, evolving-everywhere office, and take the load off of your plate. We want to help ease the burden on IT and security teams and to get you the coverage you need quickly. We recognize that, now especially, time and security are crucial.

Cybereason Remote Workforce Protection combines Cybereason NGAV multi-layered prevention, EDR analysis and response, with Cybereason MDR to manage it all for you, and remote incident response services across workstations, laptops, and mobile devices.

We know budgets and approvals are tight, so we have made this as easy as possible for your team. You can initiate deployment in 24 hours, on a flexible rate and three-month offering for fast, managed protection for remote employees. No fine print, no strings attached.

WITH THIS SERVICE, YOU GET IMMEDIATE:

- Fast, managed protection to stop advanced threats with 24/7 coverage.
- Support from a dedicated team of security experts with experience across millions of endpoints.
- Every device secured with NSS 'AA'-rated real-time endpoint protection.
- Deployment in as little as 24 hours across workstations, laptops, and mobile devices.
- Support for macOS, Windows, Linux, iOS, and Android.

Our global SOC is prepared to investigate and respond to suspicious behavior 24/7. In a time of dramatic change, where behavioral baselines are recalculated daily and security and IT staff are overwhelmed, we look to seamlessly augment your security to ensure your organization is protected beyond the perimeter.

IF YOU NEED HELP PROTECTING YOUR REMOTE WORKFORCE, CYBEREASON IS HERE TO HELP.

Read about the benefits of Cybereason Remote Workforce Protection or get in touch with one of our specialists to get started.

cybereason

ABOUT CYBEREASON

Cybereason gives the advantage back to the defender through a completely new approach to cybersecurity: the Cybereason Defense Platform. Cybereason offers managed, as-a-service, and on-premise prevention, detection and response solutions. Cybereason technology delivers multi-layer endpoint prevention by leveraging signature and signatureless techniques to prevent known and unknown threats in conjunction with behavioral and deception techniques to prevent ransomware and fileless attacks. Cybereason is privately held and is headquartered in Boston, MA with offices around the globe.

CLICK HERE TO LEARN MORE →