## Securely Maintain Business Continuity with a Remote Workforce

### Emergency Checklist

<table>
<thead>
<tr>
<th>Priorities</th>
<th>Identity</th>
<th>Remote Access</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ensure you are using strong authentication in all cases. Your source of corporate identity must be accessible securely and remotely when possible.</strong></td>
<td><strong>Consider how your team will be able to assert their identity and authorize and exercise entitlements. Implement strong identity verification and authentication techniques and enable 2 factor authentication.</strong></td>
<td><strong>Make sure your VPN configurations, policies, and software/hardware are properly configured and patched.</strong></td>
</tr>
<tr>
<td><strong>Log access to identity, both successful and failed attempts for review.</strong></td>
<td><strong>If you've adopted a non-flat network (which you should!), ensure your VPN properly segments users based on their needed network segment.</strong></td>
<td><strong>Build contingency plans if the VPN fails. An administrative backup VPN might be a good idea if no one can reach the office.</strong></td>
</tr>
<tr>
<td><strong>Consider whether you will allow insider information, source code, or strategic documents to be accessed remotely.</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### SECOPS

- 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.

- Make sure 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. More importantly, make sure they have the tools to support remotely.

- Consider mobile device security concerns that may come into play.

- Identify what data is most sensitive and prioritize.

- Consider how your employees can now exchange ideas, talk, meet ad hoc, exchange data, etc securely.

- Establish a backup communications plan that employees are prepared for in case there is a sudden event like loss of corporate email.

- Prioritize and triage: Is there a critical function or bottleneck that would hamstring the business that you can identify right now?

- Identify new functionality that has never had to leave the building before, but now does.

- Establish a support function within the security team to answer questions and help IT with an expected dramatic increase in requests.

- Think ahead: 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?

### PHYSICAL SECURITY

- Before leaving the office, make sure no confidential information is 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.
Make recommendations for employee home work environments that take security into account.

Do you have simple policies in place 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?

### AWARENESS

Encourage a refresher in awareness programs and training as people move home.

Encourage the creation of new modules around remote work given this change.

Remind your team that there are plenty of websites, including the World Health Organization's official website, where you can get all of the necessary information without having to download any “software”.

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.

Communicate with your team early and often.

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.

For more information, visit CYBEREASON.COM