Cybersecurity After COVID-19: 10 Ways to Protect Your Business and Refocus on Resilience

In the wake of the COVID-19 pandemic and the resultant implementation of social distancing directives, altered business processes, and new economic realities, businesses must review and address their technology infrastructure and cybersecurity measures.

The swift changes brought about by COVID-19 — including the movement of a large portion of the workforce to telework and the expansion of e-commerce footprints — has caused many companies to implement new IT capabilities ad hoc. Some provisional solutions have bypassed normal development, approval, and deployment processes, which have often stretched or violated existing cybersecurity policies at the same time that the activity of bad actors has increased globally.

Preparing for the Post-Pandemic World

As social distancing measures abate — and ahead of a possible second wave of coronavirus cases — organizations will need to de-risk the enterprise and adapt operations to a "new normal." This will require a thorough evaluation of pandemic-driven IT and cybersecurity changes, some of which were rapidly put in place during the response phase of the pandemic, followed by strategic adjustments of enterprise architectures, cybersecurity controls, and business processes based on long-term operating strategies.

1. Teleworking Solutions

Anticipating a permanent increase in telework, companies should consider:

- Procuring sufficient on-demand bandwidth to move content, especially video teleconferencing, across and between geographically dispersed sites.
- Establishing VPN capacity through deployment of Internet Protocol Security (IPsec)-based VPN clients or other secure connectivity solutions to employee workstations.
- Managing identity and access for a remote workforce that meets corporate security requirements and employees' ease-of-use needs.
- Implementing mobile device management solutions to address the use of company-issued and approved personal mobile devices for business purposes. In coordination, consider implementing adequate bring-your-own-device (BYOD) policies, such as those outlined below.
- Closely examining enterprise use of internet-based remote desktop protocol (RDP), which allows remote access of Windows systems and servers and is an enticing target for hackers. If its use is justified, companies should consider allowing RDP only with network-level authentication of the endpoint and rigorous patching, including the BlueKeep vulnerability on all Windows machines.

2. External Perimeter Protection

A rise in remote connections can increase a company's cyber-attack surface. Organizations may protect their external perimeters by:

- Implementing network access control (NAC) to authenticate and validate devices and enforce security policies before permitting them to connect to corporate in-office or remote networks.
- Locking down user workstations and company-issued laptops with a defined security configuration, managing configuration centrally, and not assigning administrative privileges to end-users.
- Implementing remote endpoint isolation and forensic capabilities that meet forensic chain-of-custody requirements.
- Implementing capabilities that support remote endpoint data collection and analysis to identify unauthorized activity.

3. Cloud Services

Cloud services can offer significant cost, efficiency, resilience, and potential security benefits over data storage and application hosting alternatives. But these benefits require cloud services to be deliberately and strategically adopted and managed. Companies should consider:

- Adopting formal strategies for the use of cloud services.
- Developing complete inventories of current cloud usage in the enterprise, and rationalizing the use of multiple services

0 9 9d rdp358.8635y and snpt 3.3 (i)45 (i)-0.8 (f6

4. Secure Collaboration Tools

A New Focus on Resilience

Today's IT and network capabilities have enabled the strategies that have kept many companies afloat during the pandemic. The current crisis, however, has highlighted the need to prepare for serious business disruption. A recent survey found that more than a fifth of organizations have shopped for new security solutions or services to respond to their new reality.

Organizations should consider blending new cybersecurity investments with enhanced cyber insurance coverage to reduce their retained risk, optimize spending relative to