protiviti®

Face the Future with Confidence

COVID-19: Cyber Defense and Resilience during remote operations

Internal Audit, Risk, Business & Technology Consulting

COVID-19: Social Distancing and Work Place Disruption

The business world is in a defensive huddle to take on nature's version of zero-day malware in the form of COVID-19. The pandemic has brought many businesses to a halt. The effects of social distancing and travel restrictions are having an unprecedented impact on the operating model of organizations and forcing a severe disruption to the workplace. The key operational result due to the need for social distancing is the need to rapidly implement Work From Home (WFH) models for their employees as governments of the world are forced to enforce lockdowns in the interest of public health and safety.

WFH: a paradigm shift in the way the businesses will operate

WFH enablement by the CIO's and CTO's is a strong response to encourage social isolation and to win the war against community spread of COVID-19. Enablement of the WFH model will mean that board members, employees, and business leaders will need access to a wider range of applications/ systems to ensure minimal disruption to the business. Some aspects that CIO's and CTO's need to be cognizant while implementing and sustaining WFH include:

Building computing resilience: availability of endpoint devices to employees for WFH or enabling mobile-based access to critical devices.

Remote access is the order of the day: sufficiency of licenses for technologies like VPN clients, virtualization systems, and cloud-enabled applications.

Outage proofing infrastructure: ensure vendor support to service on-site hardware in case of outages.

Disruption free transacting: Access to systems on a need to do basis: the key for businesses to remain disruption-free, is to ensure that business teams are given access to the right systems, at the right level, within an approved framework.

Some of the applications that may require access (depending on the industry sector) are:

- Core operations applications (ERP/CBS/others depending on the sector)
- CRM's and SRM's to ensure customers and vendors can operate without the need to visit offices physically
- Online banking to ensure supply chain vendors can operate
- Production planning systems and factory automation systems
- Security monitoring systems (network and physical)
- Server and network infrastructure for office communications & business collaborations

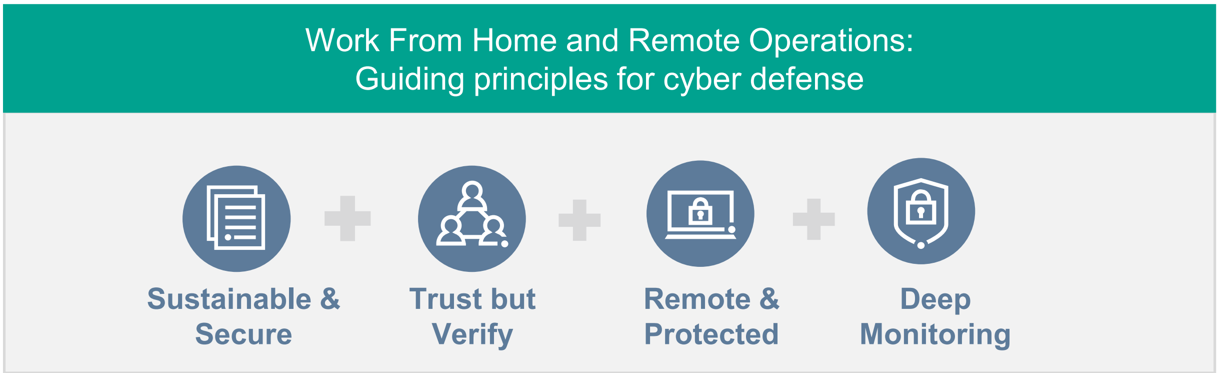
COVID-19 response: Treading cautiously on a path riddled with cyber risks

As businesses wind down their operational intensity to adapt to new methods of operations, cyber threats to organizations will remain persistent. They will be tailored to become more thematic to the evolving situation. Some of the threats, which may develop in this situation and require security monitoring teams to be extra vigilant, can be summarized as:

- COVID-19 themed phishing emails (sent to employees or end customers with themes around misinformation campaigns, false links, internal bulletins, aimed at credential extraction/ harvesting)
- Employee end point compromise/ outages/ disruptions
- Malicious remote access to IT infrastructure due to compromised endpoints
- Ransomware attack attempts on critical service providers in the healthcare and utility sector
- SCADA/ ICS attacks on manufacturing/ utility companies to cripple their operations

WFH & Remote Operations: guiding principles for cyber defense

While remote operations and WFH enablement by IT teams are needed to ensure operational resilience, the speed at which WFH is being enabled today is fraught with cyber risk, if not appropriately structured. The success of effectively designing and implementing a secure, sustainable WFH model revolves around the following cornerstone principles most relevant to IT and cybersecurity teams:


Work From Home and Remote Operations:
Guiding principles for cyber defense

- **Sustainable & Secure –** The pandemic is redefining the term "organizational perimeter". A long term perspective from CISO and CIO community will be needed to evolve the IT architecture in a manner that is cost-effective, readily available, secure, and adaptive to business growth with remote operation functionality.
- **Trust but verify –** ensure that personnel requesting remote access to the organization's assets have trusted devices that are validated adequately before granting access.
- **Remote & protected –** enable remote access in a planned and protected manner with adequate cyber defense products deployed at the endpoint and network/ link level.
- **Deep Monitoring –** with new methodologies of access and application usage, organizations need to enhance their monitoring parameters and offense detection capabilities to ensure that cybersecurity incidents do not contribute to business disruption.

Cyber defense in a remote access and WFH scenario

Cyber defense is not just about security products on systems. It involves designing a well thought out strategy that outlines a structured lock and lever mechanism to keep attackers at bay at various levels of the IT landscape.

Policy & Process

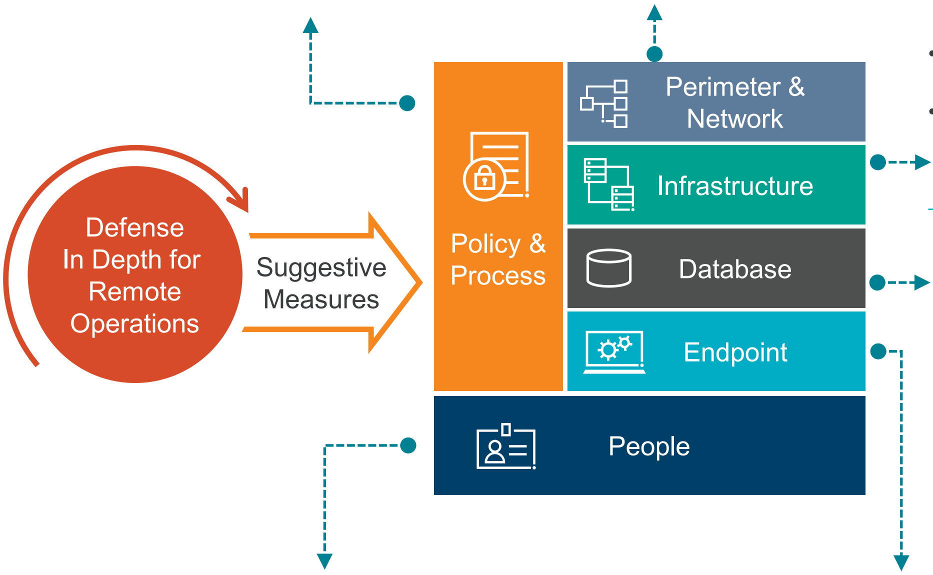
- WFH policy approved by CISO
- Remote access to critical devices/servers policy
- Inventorize all remote access, privileges, entitlements provided for easier rollback during BAU stages

Perimeter & Network

- Leverage secure VPN products
- Strict process for white list monitoring
- Remote monitoring enablement for network monitoring systems
- Ensure all network devices are patched manually or automated solutions
- Periodic update of devices for intel on COVID-19 themed attacks
- Proxy restrictions for non-business usage
- In the long term evaluate zero trusts architecture / software-defined perimeters

Infrastructure & Apps

- Access and rights on a “need to do basis”
- Avoid granting “power of God” rights remotely
- IT administrators and power users access control through PIM
- Permit remote access through company-owned/ controlled devices
- Ensure adequate WAF capacity for web-facing apps
- Evaluate implementing RASP for critical servers
- Ensure that all servers are patched manually or using patch mgt. tools remotely



Databases

- Database Activity Monitoring (DAM) remotely
- All back end access through PIM platform and via company-owned/ controlled devices
- DB’s are remotely patched using patch mgt. tools or

People: Cyber Awareness Sessions

- Create clear do’s and don'ts for all employees during WFH
- Focussed periodic alert campaigns on various threats that can hit people during WFH
  - Formal WFH training
  - Emailers and Screen savers
  - Safety guides (secure home Wi-Fi, malicious files/links, sites, apps, phishing, secure video calling etc.)
  - Helpline numbers on the intranet

Endpoints

Laptops

- EDR implementations to prevent outages on account of ransomware or malware
- Encrypted disks – to protect data in case devices are stolen
- DLP implemented to avoid data leakages and alignment to corporate proxy policies

Mobile Devices

- MDM enablement for all people accessing critical apps and server consoles through mobile devices
- Mobile device level AV/EDR/security solutions

Virtual Desktops with official email ID’s

- Evaluate virtual desktops with company-owned/controlled devices for remote contractors to ensure data stays in the corporate network

Boosting Incident Detection: Changing parameters for security monitoring

A successful cyber defense framework is not just about implementing security technology. The key element is about implementing effecting trigger and contextual monitoring mechanisms for security teams to act upon. Given the present scenario, this entails:

- Designing use cases on SIEM that are specific to the COVID -19 themes, such as -
    - Malicious remote access to key applications
    - Outbound traffic
    - Access to COVID-19 phishing sites
    - COVID-19 mass phishing mailers
    - Ransomware attempts
- Performing an external VAPT on your external footprint to plug any vulnerabilities
- Monitoring dark net for data/credentials compromise
- Heightened threat hunting to detect lurking attackers before they execute their objectives
- Evaluating options to execute a remote incident response to deal effectively with cyber attacks

Post-event horizon: a detailed stock take of unaddressed threats & impacts

WFH enablement has its challenges and consumes maximum attention. However, when the COVID-19 risk eventually dies down, enterprises need to do the following post-event activities judiciously to ensure that insider threats or/ and attackers who have stealthily opened back doors are detected:

- Immediate revocation of remote access privileges for all critical and high risks systems and devices
- Deep dive into non-investigated medium risk alerts from security systems
- Deep dive threat hunts to detect potential threats in the environment that could have been missed during crisis time operations
- Carry out compromise assessments
- Lessons learned - sessions between IT and security teams on what could have been done better

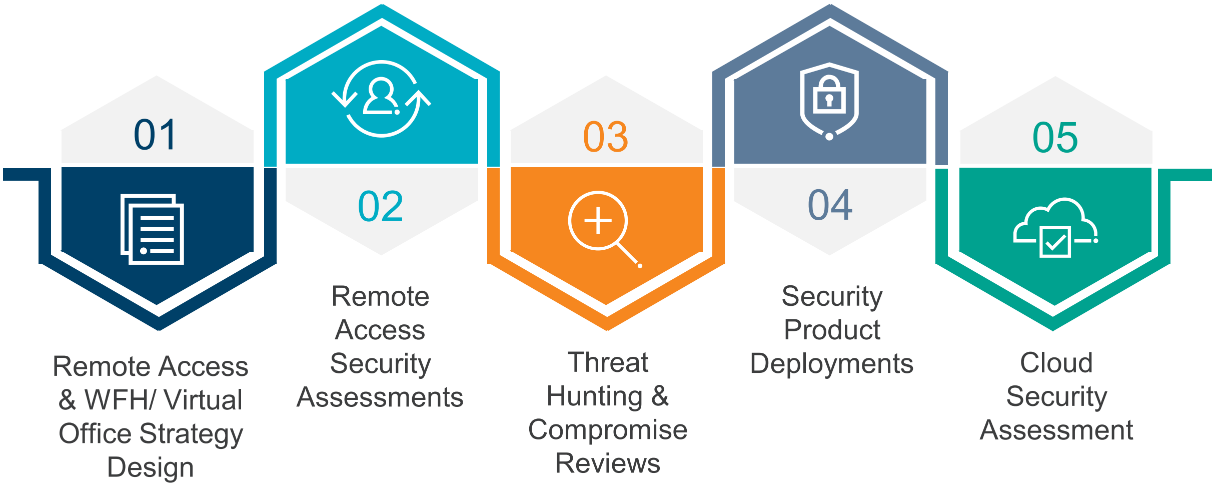
Conclusion: Cybersecurity a vital cog in the wheel of business operations

As technology seamlessly integrates with business, cyber security is an important cog in the wheel of business operations, which, if ignored at any stage, could lead to a severe impact on the resiliency of businesses that are now making a paradigm shift in the operating model.

How can Protiviti help?

Protiviti helps organizations answer the tough questions on cybersecurity around remote operations and Work From Home (WFH). Our host of services can help organizations manage cyber risk effectively.

Some of our services that we can assist security teams with are:



01 Remote Access & WFH/ Virtual Office Strategy Design

02 Remote Access Security Assessments

03 Threat Hunting & Compromise Reviews

04 Security Product Deployments

05 Cloud Security Assessment

Contact us:

Prashant Bhat
Managing Director, Security & Privacy
Tel: +91- 93222 83145
Email: prashant.bhat@protivitiglobal.in

Sandeep Gupta
Managing Director
Tel: +91 22 6626 3311
Email: sandeep.gupta@protivitiglobal.in

Our India offices

Bengaluru
77° Town Centre, Ground Floor (East wing)
Building 3, Block B, Divyasree Technopolis
Yemalur, Bengaluru – 560 037
Karnataka, India
Phone: +91.80.6780.9300

Delhi NCR
15th Floor, Tower A, DLF
Building No. 5, DLF Phase III
DLF Cyber City, Gurgaon – 122 002
Haryana, India
Phone: +91.124.661.8600

Kolkata
PS Srijan Corporate Park
Unit No. 1001, 10th Floor, Tower - 1
Plot No. 2, Block - EP & GP, Sector-V, Bidhannagar
Salt Lake Electronics Complex, Kolkata –700 091
West Bengal, India
Phone: +91.33.6657.1501

Chennai
4th Floor, A Wing, Alexander Square
No. 2, Sardar Patel Road, Little Mount
Guindy, Chennai – 600 032
Tamil Nadu, India
Phone: +91.44.6131.5151

Hyderabad
Q City, 5th Floor, Block A
Survey No. 109, 110 & 111/2
Nanakramguda Village, Serilingampally
Mandal, R.R. District, Hyderabad – 500 032
Telangana, India
Phone: +91.40.6658.8700

Mumbai
1st Floor, Godrej Coliseum
Unit No 101, B Wing
Somaiya Hospital Road
Sion (East) Mumbai – 400 022
Maharashtra, India
Phone: +91.22.6626.3333

This publication has been carefully prepared, but should be seen as general guidance only. You should not act or refrain from acting, based upon the information contained in this publication, without obtaining specific professional advice. Please contact the persons listed in the publication to discuss these matters in the context of your particular circumstances. Neither Protiviti Inc. or its Member Firms, nor the shareholders, partners, directors, managers, employees or agents of any of them make any representation or warranty, expressed or implied, as to the accuracy, reasonableness or completeness of the information contained in the publication. All such parties and entities expressly disclaim any and all liability for or based on or relating to any information contained herein, or error, or omissions from this publication or any loss incurred as a result of acting on information in this presentation, or for any decision based on it.

protiviti