Shared Services Forum

Cyber Resilience - Contemporary once again for Managing Data Protection post-Pandemic

August 28, 2020

CO-CREATE TO OUTPERFORM

WNS

Sudden Emergence of Work from Home Environment Caused by the Pandemic

- Challenges / Risks

- Cyber Security Risks
- Continuity Risks
- Operational Risks
- Impact on Collaboration
- Knowledge Management
- Impact on Productivity
- Morale and Motivation
- Overworking / Unplugging

- Managing Remote Workforce
- Credit Risks
- Regulatory Risks
- Health & Safety
- Sudden Volume Variability
- Interpretative Governmental Orders
- Privacy Risks
- MIS / Data Risks

Rapid Operations Delivery Model Inversion

Pre-COVID Operating Environment

- Hardened end-points in secure Offshore Delivery Centers (ODC) accessible for service delivery only to employees belonging to a particular client program
- No access to data storage and transmitting devices for employees in the operating environment
- Access to client applications only through secure and high bandwidth MPLS connection to client data centers. IP whitelisting at the client data center for in-bound connections for our employees
- Highly regulated access to the internet through a secure proxy solution and highly restricted email access and sending right for employees
- Internal systems not reachable from the internet and protected by layers of security
- Highly supervised environment with electronic and manual oversight
- Well designed system logging, correlation and analytical routines for early breach detection

Post COVID Operating Environment

- Secure ODCs were closed overnight due to government enforced lockdowns in most geographies and almost simultaneously
- Regulations existed that disallowed / disincentivized WFH in some geographies
- Operational delivery models involved using hardened non-portable computing devices (desktops)
- Employees able to access systems and data in an unsupervised environment
- Most employees did not have high-speed internet connections (>10Mbps) at home nor the infrastructure for home working, including stable power supply
- Access had to be enabled to client application systems through using the internet and not through secure MPLS circuits
- Our IT architecture was designed for secure in-premise service delivery model and not for a WFH environment

Key Success Factors – Enabling WFH at scale during a pandemic

1. **Strong Business Continuity programs** – enabled for early tracking of the COVID-19 outbreak and advance planning
2. **Stakeholder transparency** – ensure that all stakeholders understand **residual risks** appropriately in a WFH environment
3. **Carry forward as many technical security controls** existing in the in-premise end-point architecture deployment when architecting for remote working solutions. Add security to allow for secure remote engagement with client systems (VPN + MFA, ZT, DLP, VMDR etc).
4. **Balance between security and other risks** –remote working environment for most organizations was borne out of crisis and not strategy. A difficult balance had to be drawn between security and operability while maxing out our monitoring controls
5. **Employee training** assumed even more importance in a remote working environment where F2F team messaging is not possible. Humans are the **weakest link** in the information security chain
6. **Enabling infrastructure at home (internet and power)** assumed tremendous importance from user experience as well as enabling information security.
7. Design **log capture and correlation analysis** for new systems as they are introduced into the Hybrid Tech Model architecture for supporting the security monitoring activities
8. **Strengthen your SOC** – An organization is most susceptible to attacks during a crisis as has been visible in the current environment. Integrate **multiple threat intelligence feeds** that provide timely inputs for correlation of threat events in a distributed operating environment and allow for evasive action to be taken.
9. Lastly, **Architect for the future** – a Hybrid Tech Model to **support multiple combinations of workspace / workers** (in-premise / hybrid agents and full-time employees / part time subject matter experts)

WNS

CO-CREATE TO OUTPERFORM

This presentation and any files attached and/or transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. No part of this presentation may be given, lent, resold, or disclosed to any unintended recipients or exploited for any commercial purposes. If you are not the intended recipient and you have received this presentation in error, please return this material to the sender immediately and forthwith delete and destroy the presentation including any copies thereof from your records. We hereby notify that disclosing, distributing, copying, reproducing, storing in a retrieval system, or transmitting in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, or taking any action in reliance on the contents of the presentation in its entirety or any part thereof is strictly prohibited without the prior written consent of WNS, such consent being given at the sole discretion of WNS. Any views or opinion expressed in this presentation are those of the author and do not necessarily represent that of WNS. WNS makes no representations and to the full extent permissible by applicable law, WNS disclaims any warranties of any kind, express or implied, including any warranty of merchantability, accuracy, fitness or applicability for a particular purpose, and non-infringement of third party rights, as to the information, content and materials.

WNS.COM

WNS