

#WorkFromAnywhere


OPERATIONAL THREAT MODEL

THE REMOTE-WORK LANDSCAPE HAS BEEN STEADILY GAINING GROUND OVER THE PAST DECADE AND ESPECIALLY NOW WITH COVID-19 PANDEMIC, IT HAS FORCED MANY ORGANIZATIONS TO ACCELERATE THEIR PLANS FOR A #WORKFROMANYWHERE PRACTICE.


SUCH PRACTICE MAY HELP IN ENSURING BUSINESS CONTINUITY, PRODUCTIVITY AND COST-EFFICIENCY. BUT, IT CAN ALSO BRING ALONG UNFORESEEN CHALLENGES THAT INHIBIT THE ABILITY OF AN ORGANIZATION TO OPERATE IN A DESIRED #WORKFROMANYWHERE OPERATIONAL MODEL.

IN ORDER TO ADAPT TO A REMOTE AND DISTRIBUTED WORKFORCE, ORGANIZATIONS NEED TO FOCUS ON PROTECTING IDENTITIES AND APPLICATION REGARDLESS OF WHETHER THEY ARE IN THE CORPORATE NETWORK OR CLOUD. BY IMPLEMENTING THE FOLLOWING RISK MITIGATION MEASURES, ORGANIZATIONS CAN REDUCE THE ABILITY OF THREAT ACTORS ENGAGING IN CYBER ATTACKS IN THEIR #WORKFROMANYWHERE OPERATIONAL MODEL.

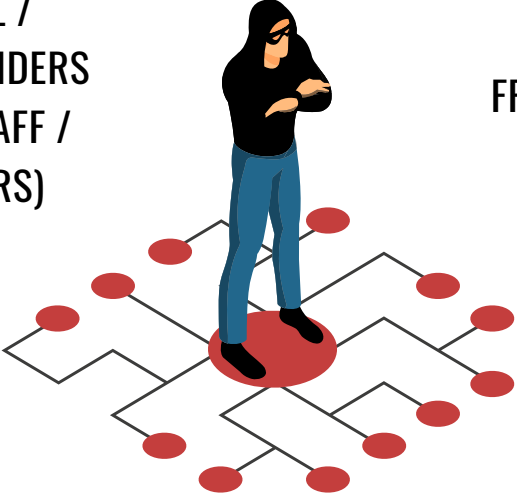
THREAT ACTORS



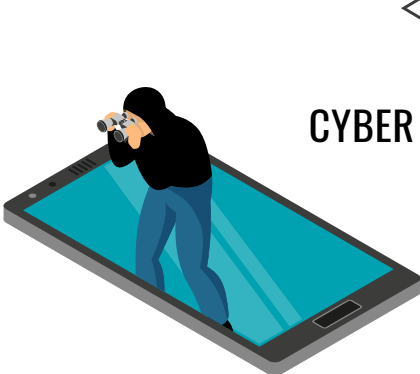
ACCIDENTAL / MALICIOUS INSIDERS (COMPANY STAFF / CONTRACTORS)




FRAUDSTERS



CYBER / ORGANIZED CRIME





STATE ACTORS



HACKTIVISTS

CYBER RISKS

- SHADOW I.T. - UNAPPROVED ACCESS METHODS
- DIRECT ACCESS (NETWORK PROTOCOLS OR EXPOSING DESKTOPS / LAPTOPS USING INTERNET-SHARING SOFTWARE ETC.)
- VPN / VIRTUALIZED DESKTOPS & ATTACKS ON AVAILABILITY
- ATTACKER LATERAL MOVEMENT
- MULTI-FACTOR AUTHENTICATION (MFA) BYPASS
- SPLIT VS. FULL TUNNEL VISIBILITY ON VPN(S)
- END-USER DEVICE TRUST MECHANISMS
- END-USER UNMANAGED DEVICE ACCESS
- LOST / STOLEN / UNATTENDED DEVICES (LAPTOPS ETC.)
- DATA LEAKAGE OWING TO INADVERTENT DISCLOSURE (ACCIDENTAL SHARING, SHOULDER SURFING, ETC.)
- UNAUTHORIZED ACCESS TO CORPORATE SENSITIVE DATA (THROUGH A SOFTWARE BUG EXPLOITATION, OR MALWARE, OR SHARED CREDENTIALS)
- PHISHING
- STOLEN / LEAKED USER CREDENTIALS REUSE



WHILE THESE CYBER RISKS APPLY TO AN ENTERPRISE THAT IMPLEMENTS #WORKFROMANYWHERE OPERATIONAL MODEL FOR ITS WORKFORCE, THE SAME RISKS CREATE AN UNLIMITED LIABILITY FOR THE ENTERPRISE WHEN THE TARGET DIGITAL ASSETS (E.G. SERVERS, DATA ETC.) BELONG TO CUSTOMERS OF THE ENTERPRISE I.E. WHEN THE ENTERPRISE EXPOSES THEIR CUSTOMERS' NETWORKS TO THESE RISKS, THE ENTERPRISE TAKES UP UNLIMITED LIABILITY.

Risk Mitigation

#WORKFROMANYWHERE OPERATIONAL MODEL

ORGANIZATIONS SHOULD BE APPLYING SECURITY CONTROLS AND CREATING THREAT MODELS FOR THEIR PARTICULAR ENVIRONMENTS NOW, AND POST COVID-19 ERA.

WHILE EACH ORGANIZATION NEEDS TO TAKE THEIR OWN UNIQUE CIRCUMSTANCES INTO ACCOUNT, THE AFOREMENTIONED THREAT MODEL SAMPLE AND #WORKFROMANYWHERE OPERATIONAL MODEL CONSIDERATIONS OFFER A STEP IN THE RIGHT DIRECTION TO KEEPING OPERATIONS BOTH SECURE AND PRODUCTIVE.

ENCRYPTED COMMUNICATION

MULTI-FACTOR AUTHENTICATION

IDENTITY & ACCESS MANAGEMENT

SECURE PRIVILEGED ACCOUNTS

DEVICE TRUST


ENVIRONMENT DRIFT

SURVEILLANCE/ LIVE MONITORING/ AUDIT


ZERO TRUST MODEL / LEAST PRIVILEGE

ACCESS CONTROL & WORKFLOW

NETWORK CONTROLS & VISIBILITY (ENTERPRISE MONITORING & DASHBOARD)



USER AWARENESS TRAINING / USER SECURITY



ARION
An Out-of-Office Secure Access Platform
for all Enterprise Digital Assets

www.silverlakesheaf.com/nebula
www.mastersam.com

© 2020 SILVERLAKE SHEAF. ALL RIGHTS RESERVED.

FIND OUT MORE