NETWORK SECURITY RISK ASSESMENT

isofy

DO YOU HAVE A PRIVATE INTERNET CONNECTION, DEDICATED SOLELY TO YOUR SPACE?

YES NO

Identify the local carriers in your area that offer dedicated internet access to your building. Request material to understand their various bandwidth options, service level agreements, and price points. Select the carrier that provides the best solution for your space based on that criteria. Work with the property owner on the ROE (right of entry) to build their fiber into the MPOE (main point of entry) within the building and extend the fiber service to your space's IT room, either through a carrier extension or a third-party.

DO YOU UTILIZE ENTERPRISE-GRADE EQUIPMENT THAT IS UNIQUELY DESIGNED FOR THE OPERATIONAL AND SECURITY REQUIREMENTS OF COMMERCIAL SPACES?

YES NO

Research each piece of equipment and understand their capabilities from a security and compliance perspective. Technical specifications such as throughput, maximum number of VLANs (virtual local area networks), and authorization policies should be explored to match the topology of the desired network you wish to provide to your members.

IS THERE A DEDICATED FIREWALL IN PLACE?

YES NO

Research the best firewall option for your space, taking into account performance, technical capabilities, and security policies. The best approach is to document the capabilities you wish to provide at your space, and work backwards from there to identify the best firewall specifications. Identifying your brand posture towards security and compliance is a first step before working towards the technical specifications. Your space should have its own firewall that is not shared by other tenants at your building so you have complete control.

IS THERE AN "ALL OUT, NOTHING IN" POSTURE IN PLACE FOR YOUR FIREWALL POLICIES?

YES NO

Identify the relevant configuration settings within your firewall policies to enable this feature. Be very cautious when performing policy changes on your firewall; any unintended change can cause your network to stop functioning.

DOES ALL OF YOUR NETWORK EQUIPMENT HAVE COMPLEX ADMINISTRATOR PASSWORDS?

YES NO

Create complex passwords for each of your network devices and store these passwords in a highly secure and encrypted platform with role-based permissions.

ARE ACCESS PERMISSIONS TO YOUR NETWORK EQUIPMENT REGULARLY REVIEWED?

YES NO

As you inevitably give various levels of access to members, vendors, and third-parties, make sure that you set a regular cadence of access reviews to revoke access and update any shared passwords. You will then need to document these changes in a change log for compliance purposes and update your encrypted password platform.

IS YOUR FIREWALL ROUTINELY UPDATED TO MITIGATE NEW AND EMERGING THREATS?

YES NO

Routinely scan for updates and subscribe to vendor communications to stay abreast of the latest releases and emerging threats. Keep in mind that some firmware releases may cause other, unintended, consequences to your network environment so it's best to confirm compatibility across your entire network stack before updating only the firewall.

NETWORK SECURITY RISK ASSESMENT

☐ YES ☐ NO IF YOU HAVE REMOTE ACCESS OR VPN CONNECTIONS TO YOUR SITE, ARE THEY SECURED WITH STRONG PASSWORDS AND ENCRYPTION?

Create complex passwords for each of your VPN connections and store these passwords in a highly secure and encrypted platform with role-based permissions.

☐ YES ☐ NO ARE YOUR WIRELESS CONNECTIONS ENCRYPTED, REQUIRING A PASSWORD TO JOIN YOUR WI-FI?

There are several ways to encrypt your wireless connections, one of the most common being a WPA2 PSK (Wi-Fi Protected Access 2 - Pre-Shared Key). Research the relevant configuration settings of your access points and enable the appropriate encryption. Note this typically only encrypts the connection between the device and the wireless access point so additional consideration needs to be given to security once connected to your wireless network.

☐ YES ☐ NO IS THERE NETWORK SEGMENTATION IN PLACE TO PROVIDE PRIVATE NETWORKS PER TENANT?

To automate the creation of private networks per tenant, select a network management partner that has the required hardware compatibility and software capabilities. The alternative is to manually provision a private network across your firewall, switches, and wireless access points each time a tenant moves in. Don't forget to deprovision that private network once they move it.

☐ YES ☐ NO IS THERE DEVICE-SPECIFIC FILTERING (LIKE MAC ADDRESS) TO AVOID UNAUTHORIZED CONNECTIVITY?

To provide this level of security, a network management partner is required. To configure these settings, a deep understanding of various network hardware, the interplay between the settings of each piece, and the appropriate protocols is required.

☐ YES ☐ NO ARE YOU ABLE TO QUICKLY, AND IN REAL-TIME, REMOVE NETWORK ACCESS FOR ANY INACTIVE OR UNAUTHORIZED USER, ACROSS ALL OF THEIR DEVICES?

Keep in mind that you can't simply change your Wi-Fi password once someone moves out of your space; that then creates an untenable change management process. You need the ability to maintain your Wi-Fi password while removing authorization from certain users and their devices. This requires in-depth knowledge and tailored solutions that a network management partner can provide.

☐ YES ☐ NO DO YOU HAVE A WIRING DIAGRAM OF YOUR NETWORK THAT CAN BE SUBMITTED AND INSPECTED BY COMPLIANCE AUDITORS?

Most compliance certifications require an updated wiring diagram of your network topology. Be sure to receive a copy of the initial "as-built" drawing from your network installer and keep that document updated if any physical changes take place.

☐ YES ☐ NO IS ACCESS TO COMMUNITY DEVICES (LIKE PRINTERS) REGULATED VIA AN ACCESS CONTROL POLICY?

To provide this level of granular shared access, a network management partner is required. To configure these settings, a deep understanding of various network hardware, the interplay between the settings of each piece, and the appropriate protocols is required.

NETWORK SECURITY RISK ASSESMENT

isofy

☐ YES ☐ NO DO YOU HAVE A NETWORK MANAGEMENT PARTNER THAT CAN PERFORM MAINTENANCE AND REPAIRS ON YOUR NETWORK EQUIPMENT?

To stay protected against emerging threats, there should be a continuous cycle of software and firmware updates to your network stack; everything from firewalls to switches to access points. This routine maintenance must be done carefully so that your network is not unintentionally affected by a version that is incompatible with your operations requirements.

☐ YES ☐ NO DO YOU, OR YOUR NETWORK MANAGEMENT PARTNER, HAVE OPERATING PROCEDURES TO REPLACE FAULTY HARDWARE TO MINIMIZE SITE DOWNTIME?

How much does 1 hour of downtime cost your business? Identify that this costs your business, both in reputation and revenue, and work to implement processes to minimize the risk accordingly. A network management partner can work with you to keep certain pieces of your hardware in inventory, and even pre-configured for a hot-swap situation. Develop contingency plans to maintain connectivity to most members in the event that certain pieces of hardware fail.

☐ YES ☐ NO IS THERE A PLAN IN PLACE FOR EQUIPMENT END-OF-LIFE UPGRADES AND REPLACEMENTS?

An end-of-life schedule should be maintained so that you are refreshing your equipment in advance of potential failure or end-of-support from the manufacturer. Remember the operational requirement of your networking equipment and accordingly plan your capital investment schedule to refresh and replace this hardware to maintain optimal performance.

☐ YES ☐ NO ARE REGULAR SECURITY ASSESSMENTS CONDUCTED ACROSS YOUR NETWORK STACK?

A network management partner can identify the required compliance tests and attestations and perform the required maintenance, scans, and penetration testing on your network so that you stay current.

☐ YES ☐ NO DO YOU, OR YOUR NETWORK MANAGEMENT PARTNER, MAINTAIN ACCESS AND CHANGE LOGS?

Each time a user is provided access to your network, and removed from your network, there should be an event recorded within a log. A network management partner with the right software solution can automate this process for you into a streamlined, and exportable, dashboard. Otherwise, be sure to export and reconcile these logs from your network equipment on a regular basis.

☐ YES ☐ NO IS THERE A DEFINED PROCESS FOR PATCH MANAGEMENT FOR ALL NETWORK COMPONENTS, INCLUDING FIREWALLS, SWITCHES, AND ACCESS POINTS?

Subscribe to manufacturer communications related to your network components and identify any emerging threats that require patch management. This often involves downloading the patch to the device and confirming functionality afterwards. Keep in mind that anytime you introduce a new patch or update, your entire network stack should then be validated to make sure that there aren't any adverse effects on performance of other components.

HOW MANY TIMES DID YOU ANSWER NO? ____

RESULTS

IF YOU ANSWERED NO...

Less than 5 times	Your network is largely secure and only requires minor changes with your network management partner.
More than 5 times but less than 15 times	Your network requires a robust assessment and re-configuration from a network management partner.
More than 15 times	You have a highly unsecure network that presents an immediate risk to your users and your business reputation.