WesTechs
PO Box 25 Midland, TX 79702

Concho Valley Immediate IT Plan – Executed
5-2020, Rev. 1
6/29/2020

Executive Summary

CSCD and CRTC ("Client") are running on old and out-of-support server hardware. Replacement hardware has been purchased but not installed at CSCD; replacement hardware is in place at CRTC but full migrations have not been completed. Network switches do not appear to have coverage from the manufacturer and no spare switches could be located. A switch or server failure would result in a widespread outage affecting multiple end users.

CSCD should contract an IT consultant or company to mitigate the risks identified below, implement and migrate new server hardware, and install previously purchased client workstations. Many IT best practices are currently lacking and, if implemented properly, will increase uptime and enhance productivity of the organization.

If Client can contract a third party to bring all IT infrastructure up to date and to best standards, one or two IT employees could be hired to manage the day-to-day tasks at the user and workstation level. The IT infrastructure could be managed, monitored and backed up by an outside IT resource.

This means Client can hire employees with smaller skill sets which are less likely to be lured away by other opportunities. Because these entry-level employees are more common than highly skilled employees, occasionally losing an employee wouldn't be overly impactful to Client; they would have an outside IT company in place for support while seeking a replacement employee.

Network overview documentation was created and provided. All identified passwords were changed placed into an encrypted PDF.

CSCD

CSCD has (2) servers that are out of warranty support and (1) network attached storage device from Synology. The DS1 server and Synology contain user data; DS1 and DS2 are domain controllers. CSDC has (2) new Dell servers that were likely planned replacements for DS1 and DS2. It is recommended to stand-up these servers and migrate the CSCD domain and all data to the new servers. Synology devices, while generally reliable, do not offer real-time support and are not recommended to be used for production data. The device should be repurposed as a backup target.

Timeclock software runs on an old workstation with insufficient hardware. It is recommended to create a Hyper-V cluster with the two new Dell servers and deploy virtual servers ("VMs") with dedicated Active Directory and Application VMs. CSCD may need to purchase new hard drives for these servers as the already purchased drives are slower, larger drives that favor capacity over performance. These slower, larger drives could be repurposed as an additional backup target or VMs with lower resource demands.

CSCD is provided an internet connection to Tom Green County. There are (2) layer 3 devices which ultimately route to the internet (a Sophos firewall and Cisco layer 3 switch). CSCD should work with County IT to resolve this routing issue to the county in order to access both county resources and the internet. Firewall rules should be added to Client's Sophos device so that unsolicited traffic from the county is rejected. Most end user machines today do not send their traffic thru the Sophos; instead it is routed to the Cisco layer 3 switch.

There is no evidence of support or warranty for the CSCD network switches (other than any "limited lifetime" warranties that the manufacturer may provide). It is recommended to obtain Cisco Smartnet for all switches or purchase several spare switches that are tested and sitting on the shelf in the event of a failure. This is especially true for the core 3750 switch; CSCD would be severely hampered if this switch were to fail.

The network configuration and routing table contains many redundant networks and routes which appear to no longer be in use. These VLANs and routes should be removed from the network configuration.

Although some backups were being performed, both production and backup data was accessible with domain administrator credentials. This means a compromise of a domain administrator account would allow a threat actor to destroy or encrypt both production and backup data. Westechs is currently proving cloud-based backups of identified data on a temporary basis. This backup data is not accessible via any CSCD account. It is recommended that Client perform backups that are onsite, offsite and immutable for proper protection.

Client workstations are configured with static IP addresses; it is recommended to migrate them to a DHCP server running on the Sophos firewall. There are numerous Windows 7 machines that no longer receive security updates from Microsoft; they should be replaced with the new workstations that were purchased but never installed.

Windows 8 and greater clients were not receiving Windows updates due to being configured to update via a non-functioning WSUS server. Changes were made to Group Policy so that all eligible clients would download and install updates directly from Microsoft. It is recommended to configure an RMM (remote management and monitoring) product, WSUS, or other update solution so that Microsoft security updates are installed and monitored each month. Up-to-date clients are vital to increase the over security posture of Client.

CRTC

CRTC has (4) servers; (2) are out of warranty and Microsoft software support. CRTC also has (2) network attached storage devices from Synology. All (4) servers are Domain Controllers. The (2) new servers are in production but there are data and applications that still need to be migrated from the (2) old servers. The (2) old servers should be decommissioned upon completion of migration.

The primary line of business application (Sentry) resides on the older servers and should be migrated to the new servers. It is again recommended to use VMs. Dedicated VMs for Sentry (and other applications) would allow the vendor direct access to their own application server but not Client server resources (as it is today).

Backups appear to be running from the old servers to the network attached storage device at the opposite facility. However, both production and backup data access is available with domain administrator credentials. Westechs is currently proving cloud-based backups of identified data on a temporary basis. This backup data is not accessible via any CSCD account. It is recommended that Client perform backups that are onsite, offsite and immutable for proper protection.

There are several Windows 7 machines that no longer receive security updates from Microsoft; they should be replaced with the new workstations that were purchased but never installed.

The male and female facilities are networked together via a wireless bridge. The original vendor and credentials for the radios could not be determined. It is recommended to either install an internet connection at both sites and create a connecting VPN tunnel or procure and configure a hot spare radio set in the event of failure. Radio failure at either end, rain fade or other environmental issues could take a facility down.

Common

The organization is licensed for PDQ; this is an excellent system administrator utility and should be retained for IT administrator use. A Ninite Pro subscription was discovered but expired; Client should renew subscription due it's low cost and ability to easily patch third party software on end user machines.

It is recommended to procure and install backup battery systems that are connected to the network in each primary server closet so that power events are communicated. Environmental monitoring should be incorporated into these systems so that alerts can be sent when there is a power outage or HVAC failure. An outside monitoring system should be used to verify the health and availability of the entire IT infrastructure and environment. Westechs is currently monitoring available items on a temporary basis.

There are numerous group policy objects on each domain performing only one or two functions. These should be consolidated and updated as necessary. Active Directory in general is fragmented and should be optimized and organized. User and computer accounts that hadn't logged in for (90) days were identified, disabled and moved to a dedicated OU for future removal.

Unifi (wireless network) controllers and access points at each site are extremely old and should be upgraded. The controllers should become Linux VMs and the access points should be upgraded to 802.11 AC.

It is recommended to add multi-factor authentication to Office 365 accounts. The 365 administrator account is also a 365 user with email functionality; it is recommended to remove the user license and modify the account to be a dedicated admin without email or other services. Multi-factor should be implemented on the administrator account (at a minimum).

Items Performed

- Network
  - ✓ Change password on firewall, routers, and switches
    - Changed and supplied
  - ➢ Perform audit of perimeter firewalls and mitigate immediate risks
    - No outside ports/services found
  - ✓ Perform configuration backup of all known and discovered network equipment
    - Captured and supplied
  - ✓ Implement active monitoring for network and server infrastructure
    - Implemented for DS1, DS2 and Synology
    - Implemented for MALECCF-DS1

- Servers
  - ✓ Change domain administrator password
    - Changed and supplied
  - ✓ Identify other domain administrator equivalent accounts and disable/change passwords
    - Changed and supplied
  - ✓ Identify and disable/change remote control and remote access products
    - Disabled Teamviewer service accounts on servers; changed Teamviewer account password
  - ✓ Verify/install current Windows security patches
    - DS1 set to Sat schedule; DS2 up to date; clients pointed to non-functioning WSUS server – adjusted GPO to allow internet-based updates
    - CRTC default configuration of internet installation
    - (2) 2008 R2 servers at CRTC unable to be patched
  - ✓ Identify and backup data to immutable cloud servers
    - Backed up DS1 data, DS2 full, Timeclock full, (1) Synology
    - Backed up MALECCF-DS1 data, (2) Synology
    - Backed up MALECCF, FEMALECCF

- Client
  - ✓ Verify/install current Windows security patches
    - WSUS at CSCD not functioning and used by GPO; pointed clients to Microsoft for updates
    - CRTC pointed to internet (default configuration)
  - ✓ Verify/install current 3rd party software patches
    - Patched (two passes)
  - ✓ Identify and disable/change remote control and remote access products
    - See Teamviewer notes; no other remote access found
  - ✓ Verify functionality of anti-virus software
    - Yes; recovered and supplied Sophos credentials
  - ✓ Verify location of client data (local vs server); create plan to relocate if necessary
    - Redirection to servers; backed up
  - ✓ Locate unsupported software and software with vulnerabilities; mitigate or present mitigation plan
    - Discovered software current and/or patched

- Software
  - ✓ Identify line of business applications; develop primary and backup access plans
    - Timeclock; remainder are cloud-based
    - CRTC - Sentry

- General
  - ✓ Identify, mitigate and/or document IT risks
    - All sites: domain controllers sharing other roles (file sharing, DHCP, etc)
    - All sites: domain controllers/servers running on end of life hardware (CSCD)
    - All sites: clients have static IP addresses
    - CSCD: WSUS not functioning
    - All sites: Excessive GPOs
    - CSCD: Extremely old Unifi controller
    - CSCD building appears to be run on single access point
    - All sites: Data located on Synology devices
    - Ninite expired
    - All sites: Windows 7 clients need replacement
    - Timeclock running on old PC
    - CRTC router requires local password reset
    - No credentials/config backup/spare equipment for wireless bridge between male/female facility
  - ✓ Create baseline network documentation
    - Created and supplied
  - ✓ Change passwords of all known external systems and websites
    - Changed and supplied