Rapid freight converged network security

Technology, Information Technology

Rapid Freight Converged Network Security

Implementation of a converged network system is the key adjustment that the CIO of Rapid Freight should consider. The network system merges phone, voice, and data services under one platform. The network will boost portability of technology by enhancing the use of Personal Digital Assistants and soft phones. The network will also enable ease of monitoring all aspects of the organization while reducing challenges in security (Paul, 2011).

Implementation of the system introduces some security challenges. If a threat penetrates the network, it will easily infiltrate across the domain due to the single line flow. The challenges are both external and internal to the organization. External challenges arise from unauthorized software or data that seek entry into the organization’s domain. Internal challenges, on the other hand, can be either accidental or intentional. Accidentally, internal threats occur when people use their portable devices outside the network then plug them back in importing viruses and other malware. Some members of staff might be malicious and try to access unauthorized segments (Paul, 2011).

External threats are easily kept at bay through the implementation of firewalls. A firewall allows flow of data from known sources to the webserver or specified destination while rejecting unknown traffic. If the firewall is compromised, it severs the connecting of the system to the internet host. Notwithstanding, firewalls are not perfect and should not be used solely (Stewart, 2010).

Unified Access Control and Network Access Control ensure that device users are authorized to use the network. Account management system registers

network users and signals any illegal activity. Coupled with Personalization, the intervention will keep the network safe from internal threats of any nature (Gregory, CISA, & CISSP, 2007).

Implementing session management features such as Virtual Private Networks (VPNs) will overcome challenges posed by use of VoIP phones, Video conferencing and PDAs. IPSec VPN scrambles traffic from the phone and safely connects to the corporate network without fear of infiltration. Soft phone users will require authentication into the Converged network. Secure Socket Layer VPN (SSL VPN) ensures that users are logging in from healthy computers when accessing the network remotely. Intrusion Detection and Prevention software (IDS and IPS) will further enhance overall security by scanning entire network to identify and report signatures or suspicious traffic arrays (Gregory et al, 2007).

Figure 1. Security measures framework. This figure illustrates how various security measures will be incorporated into the proposed Converged Network

References

Gregory, P. H., CISA., & CISSP. (2007). Converged Network Securities for Dummies. Hoboken, NJ: Wiley Publishing Inc.

Paul, S. (2011). Digital Video Distribution in Broadband, Television, Mobile and Converged Networks: Trends, Challenges and Solutions. Hoboken, NJ: Wiley Publishing Inc.

Stewart, J. M. (2010). Network security firewalls & VPNs. Mississauga, Ont: Jones & Bartlett Learning.