REDSHIFT
NETWORKS
Secure Cloud Communication and Collaboration.

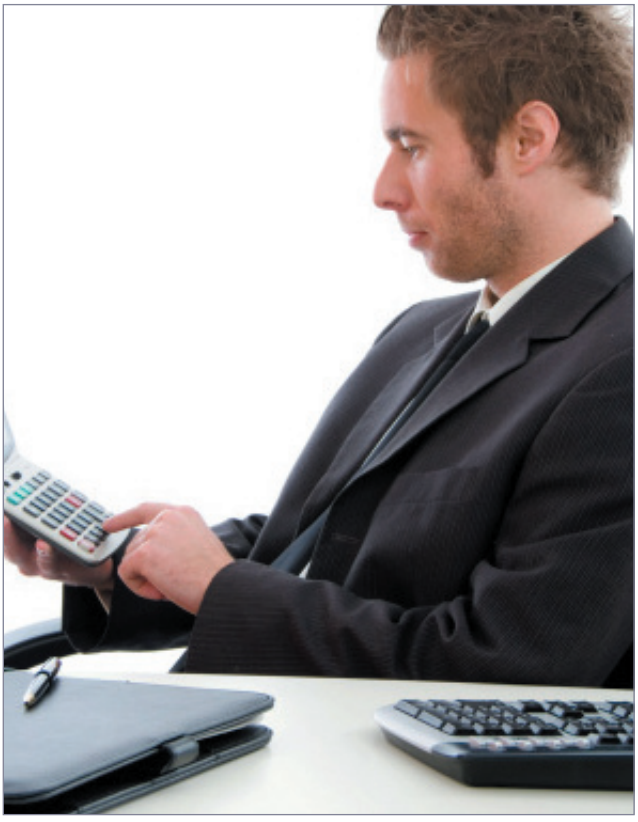
Unified Communication Services

Financial Risks of Cyber Threats

A primary and critical consideration Chief Information Officers and Chief Operating Officers deploying hosted VoIP (Voice over IP) and Unified Communications (UC) must consider are the cyber threat risks inherent in new IP-based services.
The economics of hosted services are driving double-digit growth and expectations for security and reliability must keep pace. VoIP and accompanying Unified Communication services, such as messaging and video collaboration, are crucial business applications. Security breaches; including service disruptions experienced by the customer, will result in loss of revenue from unauthorized use, Denial of Service (DoS), information theft, and intangible loss due to reputational damage and unavailable network resources.

Typical ROI analysis can provide valuable insight for decision makers when assessing the benefits of VoIP/UC security. However analysis alone is insufficient. Rather, business decisions should be made based on security as a risk reduction requirements, much like disaster recovery and redundant power. In the end security measures should result in senior management's confidence that the network is protected from intruders and that security is sufficient to prevent catastrophic loss of information, services, and reputation.

To aid in this decision RedShift Networks has developed the following risk assessment tool to provide decision makers a process for understanding the financial implications of a potential VOIP Security attack or threat to their network.



Risk of DoS/ DDoS attacks

What is the potential revenue loss to your organization when services are unavailable to your customers? Flooding attacks consisting of tens of thousands of legitimate requests coming from sources all over the world have severely incapacitated operator networks in minutes, and in several cases made it impossible for customers to access services.
The highly distributed attacks are difficult to defend against without proper threat identification and defense mechanisms in place. With the growing intensity of VoIP attacks containing malformed messages and legitimate requests, defenses must improve accordingly.

Financial losses due to network downtime:
$_____

- Industry average for the number of service-impacting events (2-6 hours of disruption) is .8 per year or 1.5 over a 3-year period.
- Customer credits issued per 8 hours of outage SLA terms or .25%: $ _____

REDSHIFT
NETWORKS
Secure Cloud Communication and Collaboration.

Risks of Theft – Toll Fraud:

Attacks against VoIP systems aimed at stealing a victim's communications capability are on the increase and still inflicting thousands of dollars in damage.
With the market demand for quickly implementing new VoIP systems, features and standards, implementation flaws are common. IP PBXs, for example, contain many potential software vulnerabilities.
Programming mistakes; such as not properly checking the size of the parameters of a protocol request, when exploited, can result in the attacker obtaining system remote access at user and management levels, leading to toll fraud, confidential information compromise/theft or DoS.
Toll Fraud continues to cost VOIP Carriers millions annually. VoIP endpoints and network components are located via SIP scans and then exploited for the purpose of stealing expensive long distance services. According to the SANS Institute an average reported toll fraud incident costs around $40,000. RedShift Networks has encountered numerous cases where a single incident resulted in $500,000 or more in cost to the provider.
Typically these attacks are set up in advance, with the fraud beginning on a Friday night and continuing through the weekend, often saturating two to four connections with calls to locations where long distance charges can run as high as $20/minute.

Financial losses from Toll Fraud: $_____

- A typical service provider experiencing a conservative 4 simultaneous calls over 48 hours X $10/minute would lose over $100.000 in revenue from a single incident.

Operational Costs

What are the operational costs incurred to mitigate a Unified Communications Services attack on the VoIP network?

Network engineering personnel costs: _____

- Average fully loaded cost is $75 per hour
- Default of 4 man-hours for small- to mid-sized hosting data centers.

Cost per help desk call: _____

- Industry average for Tier 1 help desk is $20 per call

Costs of Information Theft

Potential liability from loss of confidential information: $_____ (passwords, voice mail, etc.) plus compliance violations.

Loss of confidential information is a major issue in many industries. Trade secrets, customer information, employee listings, spoofing, and compliance regulations make information protection mandatory.

Financial Industry (GLBA)
Regulations require the some industries maintain strict VoIP security measures to safeguard confidential voice information.

In the financial industry, sensitive information has to be protected and GLBA requires that financial institutions investing in VoIP gear ensure that "Proper VoIP security mechanisms" are implemented.

Healthcare Industry (HIPAA)
In the healthcare industry, HIPAA, also requires that healthcare institutions safeguard the confidential patient data in voicemail and other VoIP enabled systems.

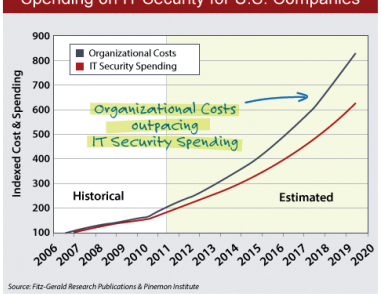
PCI Standard – Credit Card process (Retail)
The self-imposed PCI standard requires that all companies doing business with VISA or MasterCard also have strict application aware VoIP Security.

Using the Cost Assessment Tool

This model is designed to assist service providers to project the ROI of security expenditures and the revenue protection based on growing mitigation costs.
Using data provided by Fitzgerald Research Publications and The Ponemon Institute the chart shows that U.S. firms are now losing more money to operational costs of cyber attacks than they are spending on security.
In other words, effective threat management systems pay for themselves. By utilizing industry data for cyber attacks, your own financial data, the model's results will demonstrate the positive ROI, customer revenue protections, and lower financial risks that will be gained from an investment in a comprehensive UCTM solution from Redshift Networks.

For additional information on the RedShift Network Unified Communications Threat Management solution visit www.redshiftnetworks.com.

Organizational Costs of Security & Data Breaches for U.S. Companies vs Spending on IT Security for U.S. Companies



RedShift Networks - 4000 Executive Parkway - Suite 290 - San Ramon, CA 94583 - U.S.A.
Voice +1 (925) 272-0100 - +1 866 824 5775 (toll free) - www.redshiftnetworks.com - info@redshiftnetworks.com