ISO 27001 Information Security Management System

Solution Overview: TeleDirect Information Security

Overview

Due to growing information security risks, organizations must continually monitor and effectively manage the security of their computing infrastructure. Further, organizations must ensure the confidentiality, integrity, and availability of their information assets.

ISO 27001:2013 is a time-proven international standard of best practices published by the International Organization for Standardization (ISO) for establishing, maintaining, and improving security programs for all organizations. An ISO 27001 based Information Security Management System (ISMS) is a set of integrated processes that govern the management of security program policies and procedures. TeleDirect has achieved and continues to achieve many benefits from implementing an ISO 27001 based ISMS. We have been certified since 2007 with ISO 27001:2005 through our governing body BSI, and with the new standard now available, are currently in the process of being certified for ISO 27001:2013 with a new certifying body, A-Lign.

Designing and implementing an ISMS is a significant undertaking for security program managers. Because ISO 27001 is a multi-layered security management standard, organizations must design consistent policies and practices in order to apply the appropriate security controls required by ISO-27002 and also to prove compliance per ISO-27001 control objectives.

ISO 27001 Compliance and Certification

ISO 27001:2013 provides a security governance framework that allows us to formalize a service delivery platform that complies with all necessary controls, standards, and processes. It also provides mechanisms for third-party auditors to validate the controls, standards, processes, and operating procedures. By completing this certification in October 2016 across multiple locations, our customers have the assurance that TeleDirect uses internationally recognized best practices when securely managing security information. ISO 27001 certification is not a one-off exercise. To maintain the accredited certification, A-Lign annually conducts interim audits and a full three-year recertification of TeleDirect's Call Center. These certificates will be available on request from your team.

By currently complying with the controls specified by the ISO 27001:2003 standard during this transition, organizations can be confident that TeleDirect has incorporated a standard code of practice that:

- Is recognized by partners and customers as a best practice security management system
- Enforces ongoing reviews to drive continuous improvement to the security management system
- Ensures that information security activities are recorded and are auditable
- Raises the level of security and awareness of best practices through continuous training
- Meets customer contractual and service level requirements for ISO 27001 compliance
- Minimizes the need for their customers to allocate time, budget, and resources to conduct independent audits.

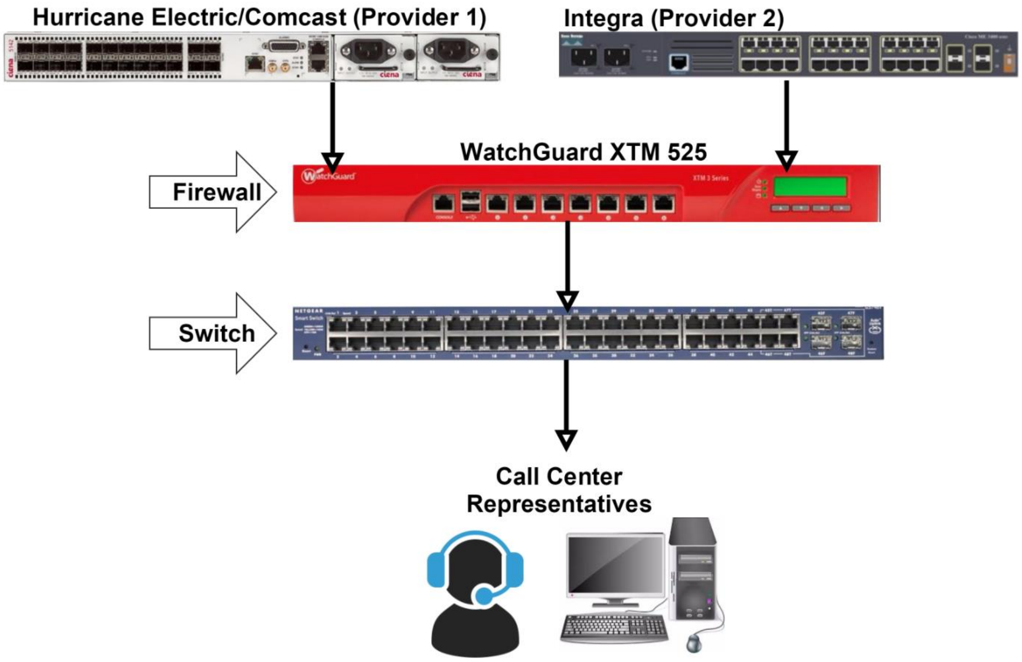
Network Security

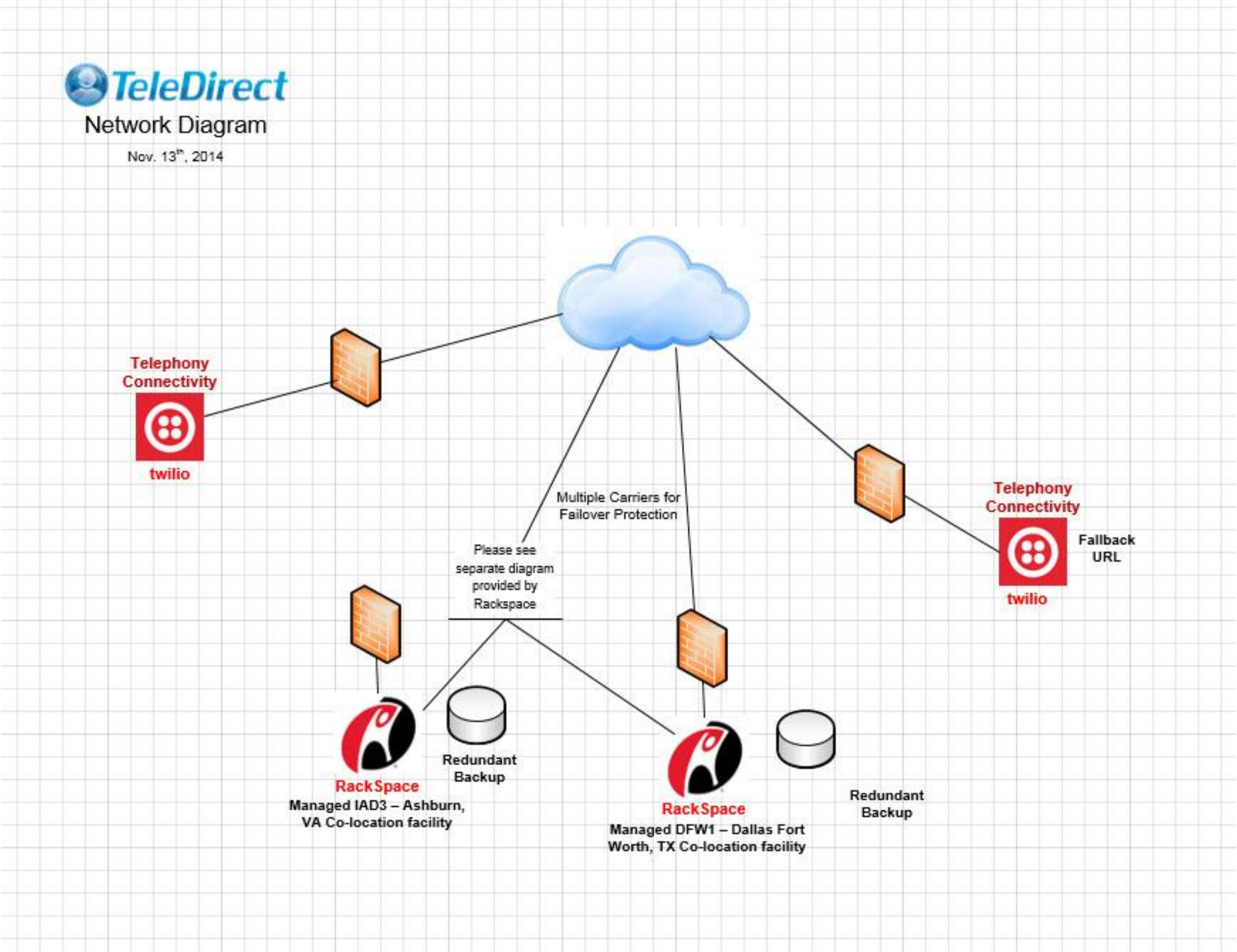
TeleDirect's objective of robust network security is to ensure that its core and supporting business operations operate securely with minimal disruptions. As requested, the following answers will provide additional insight and knowledge regarding the proactive steps we take to mitigate possible network vulnerabilities.

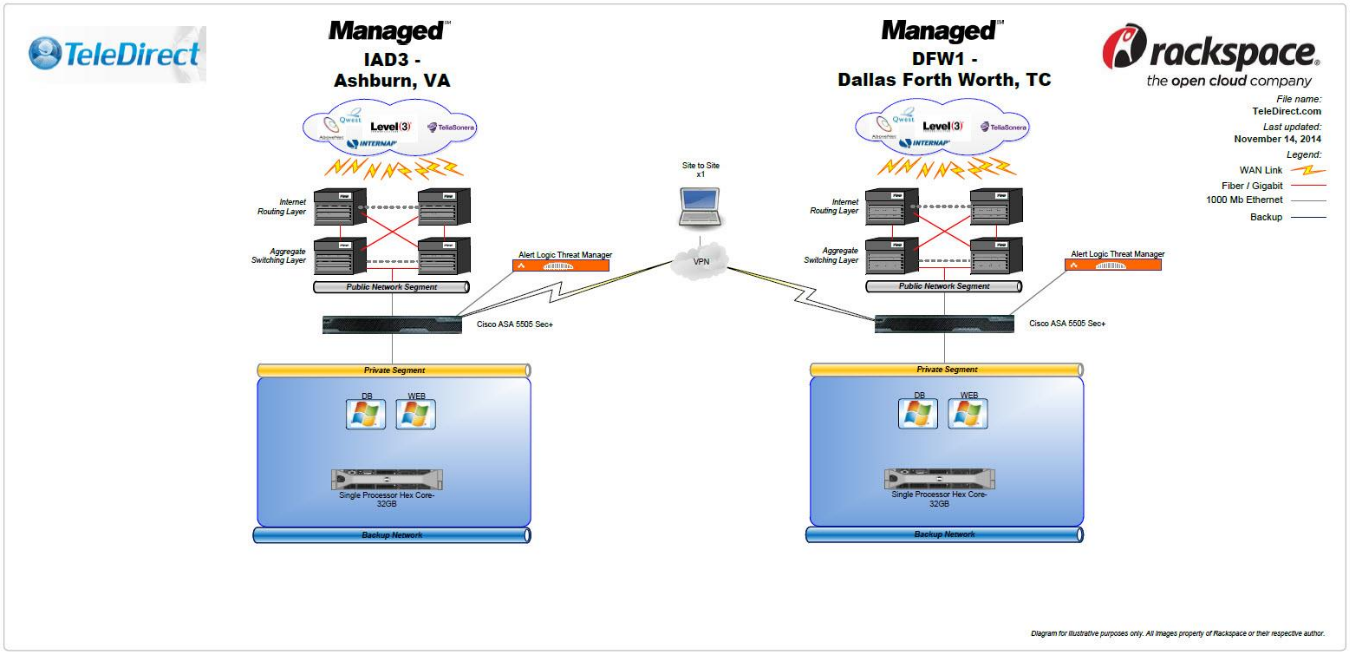
1. ***Why do we believe our network is secure?***
   Our network is secure due to our redundant security protocols being monitored 24/7/365. Upon entry of internet connectivity within our network and premise, all data is parsed through one of two firewalls, with two internet service providers being utilized to ensure redundant connectivity. Both providers go through their separate firewalls (XTM 525). Please refer to the network diagram below.

2. ***Why are we not vulnerable to outside attacks and security threats?***
   Despite every security measure in existence, ANY network connecting to an external WAN (the internet) is susceptible to intrusions. However, as is the industry standard, we have employed both a hardware and software firewalling solution provided by WatchGuard, with Intrusion Detection rules and restrictions established for incoming and outgoing traffic governing both http and https protocols.

3. ***How can we access client network without violating their security?***
   With Tata Communications providing us either unique credentials or ip address/port information already configured for our usage, our authentication access does not violate client security as we are a true extension of Tata Communication business and security adherence and compliance requirements.


Hurricane Electric/Comcast (Provider 1)
Integra (Provider 2)
WatchGuard XTM 525
Firewall
Switch
Call Center
Representatives


TeleDirect
Network Diagram
Nov. 13th, 2014
Telephony
Connectivity
twilio
Multiple Carriers for
Failover Protection
Please see
separate diagram
provided by
Rackspace
Telephony
Connectivity
Fallback
URL
twilio
RackSpace
Managed IAD3 – Ashburn,
VA Co-location facility
Redundant
Backup
RackSpace
Managed DFW1 – Dallas Fort
Worth, TX Co-location facility
Redundant
Backup



Data Security & Confidentiality (Printer & Hardware Limitations)

Each employee is given access to systems based on the demonstrated needs of his or her position. Systems and applications have several pre-defined groups to which employees may be assigned. The following table illustrates the application and levels of access:

Department Designations -
(A)Customer Service Representative
(B)Team Lead
(C)Management
(D)Accounting
(E)IT

Points of Access -

Station:	A,B,C,D,E
ACD:	A,B,C,E
Dashboard:	A,B,C,D,E
Accounting:	D,E
IT:	E

Access Groups

There are five access groups at Tele-Direct, each with different levels of access across the organization. At the level of CSR, an individual has access to use a workstation, log into our ACD to take phone calls, and may access a personal dashboard to review performance metrics. Workstation access does not allow general web surfing (due to software controls in place) nor does a user have access to the operating system. There is no email nor printer access.

At the Team Lead level, an employee has the same access as a CSR, with the addition of an Supervisor View that allows the user to view current call activity as well as current employee activity. Dashboard web portal access allows Team Lead members to provide customer service to a client by reviewing their script, their lead management, and other services they may have purchased. The network drive is shared across the organization and is password controlled. The network drive is used to share project information so that location is less relevant than access level.

At the Management level, an employee has the same access as a Team Lead, with the addition of Dashboard web portal access both internally and remotely. This access allows a member of management to provide customer service to a client by reviewing their script, their lead management, and other services they may have purchased.

There are two other areas of information that are not available throughout the call center: IT and Accounting. These are compartmentalized and only those people who are employed in those departments have access to that information. Access is controlled by physical (locks) and software (password) controls.

Upon hiring, HR assigns a new employee a unique log-in and password to access the OpsCenter and retrieve personal performance information only from his or her dashboard.

During new hire training, a new employee is trained on the proper use of his or her log-in, and are provided with a job aid explaining the proper use of the system.

When an employee advances from the position of CSR to Team Lead, access levels are changed by Operations management once confirmation of the new status is confirmed with the Operations Manager.

When an employee ends his or her employment with TeleDirect, the user account created for the employee is deleted and a record is kept in the employee file confirming the removal of access rights.

At least two times per year, Operations will prepare a report for management confirming the proper assignment of access levels.

Data Security & Confidentiality (Secured Documentation within Premises)

TeleDirect is a secure Call Center; therefore, we have policies in place that are designed to keep our Clients data safe from fraud. Protecting our Clients data is a top priority as we continue to be successful.

We maintain a secure environment where our Customers data is protected from fraud. We have taken the necessary steps to secure our network so our Call Center floor must follow suit:

1. No Pens, pencils and/or any other writing instrument are allowed on the operations floor.
2. No cell phones are allowed on the operations floor, regardless of whether they are turned on or off.
3. No purses or backpacks are allowed on the operations floor.

Since these all present a security risk to our Clients data we have to adopt a zero tolerance policy.

TeleDirect also enforces a clean desk policy to protect all non-public information at our location. Upon leaving a workstation, each employee must execute a Leaving Station application to lock the system and clear the screen.

This clean desk policy extends to Management as well. At the end of every work day each Manager is required to have a desk free of all non-public information. Any such information must be in a locked drawer. We monitor all staff to ensure every member of management is compliant with this policy. As part of a daily inspection, the ISR documents any violations of this policy, where a Security Incident is completed for any offenses.

Password Protection

The scope of our policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any TeleDirect facility.

- All system-level passwords are changed on at least an annual basis.
- All user-level passwords (e.g., email, web, desktop computer, etc.) are changed at least every nine months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "Team Lead" have a unique password from all other accounts held by that user.
- All user-level and system-level passwords must conform to the guidelines described.

Our passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9,!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long (9 is strongly recommended).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.