Collecting Huge Amounts of User Data Telco Technology

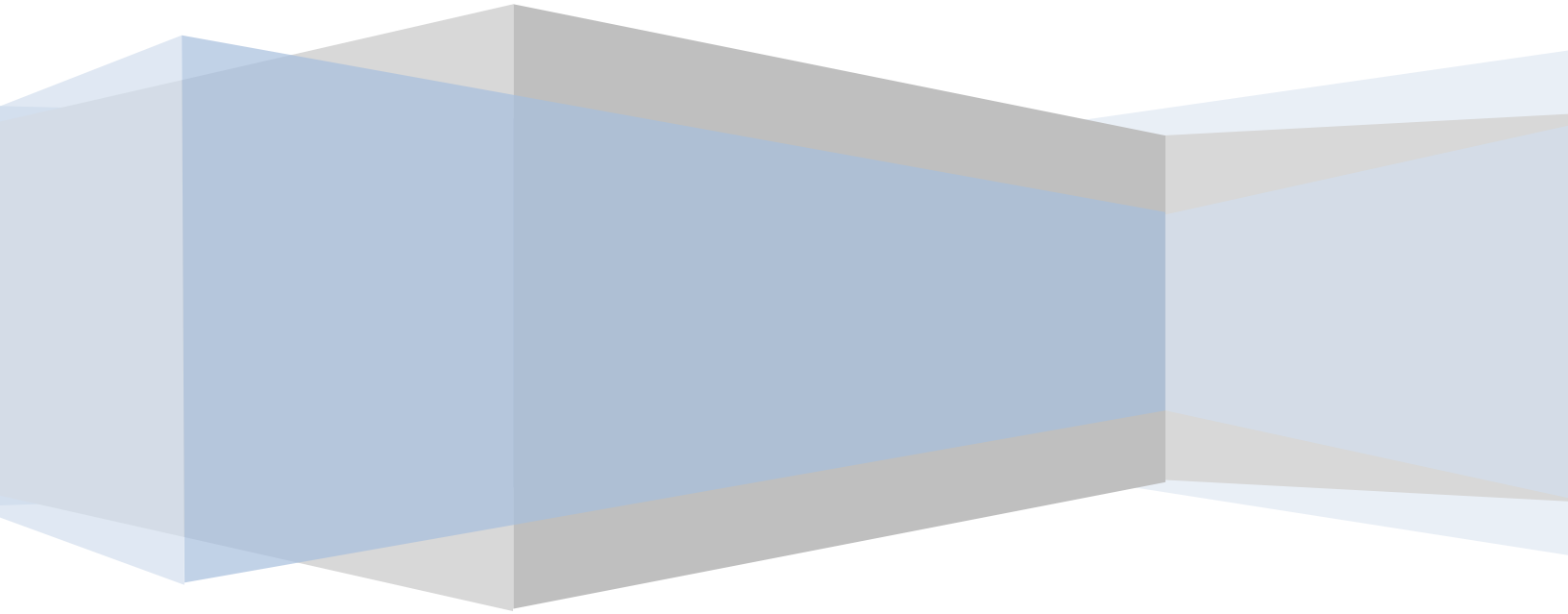
IT Security Policies and Procedures (MITS 5600G)

Ben Yankson

Cate Dillon

Dev M. Devendra

Muath Al-Badawi



DEC-2012

Security Policies & Risk Mgmt (MITS 5600G)

Group Project: Collecting Huge Amounts of User Data

Telco Technology Summary and CDR related Information Security and Business Impacts

Author: **Dev M. Devendra**, ACMA (UK), CGMA, PMP

Background

A telephone company also known as a **telecommunications service provider** provides telecommunications services such as telephony (voice) and data communications services. They include monopoly local exchange carriers, competitive local exchange carriers, and mobile wireless communication companies. Examples of such companies in Canada include Bell Canada, Telus, Rogers Communications and Fido to name a few.

Telcos collect, process and use of large amounts of user data as part of their daily business operations which are critical to their ongoing ability to provide uninterrupted and quality products and services to their subscriber client base including ensuring data accuracy and timeliness of their revenue collection processes and financial integrity.

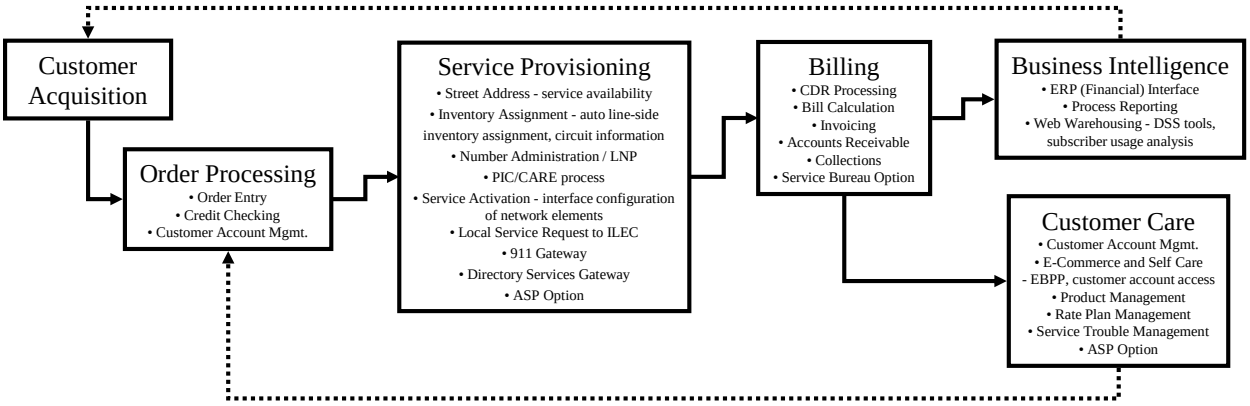
As per the 2011 BCE Inc. Annual Report, Bell Canada had 7,572,651 wireless subscribers and 8,730,431 local telephone subscribers, many of whom also use Bell Canada long distance voice services [1, p2]. Each of these subscribers (individual consumers and business) makes tens, hundreds and some even thousands of wireless and wireline phone calls on a daily basis. This represents a very large amount of data, an estimated over 100 Billion **Call Detail Records (CDR)** annually, of subscriber service usage which are collected, processed, stored and used by Bell.

Summary of Telco Processes and Technologies related to Revenue Management

Telco **Operational Support Systems (OSS)** and **Revenue Management Systems** which includes switches, collector, billing and invoicing systems are used to generate and process large amounts of CDR data.

Call Detail Records are initially generated by a **Telco Switch** when a subscriber or user of the telecommunication service initiates a telephone call or other service usage. A telco company may install and use several types of switches within their network infrastructure environment. Each of these switches may have a slightly different CDR format although they tend to collect the same type of network usage information. The CDRs from these switches are then passed on to a **Collector System** whose primary function is to standardize the information coming from multiple switch CDR formats. The standardized CDR is then passed on by the Collector System to the Billing System for further processing.

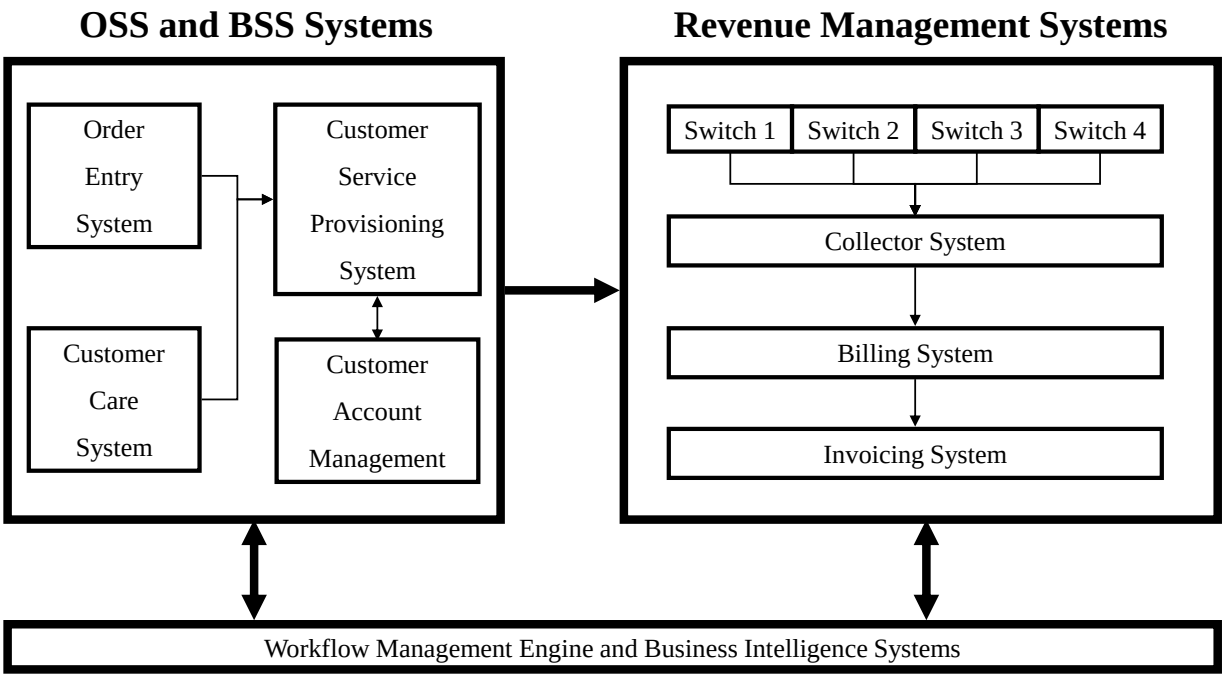
Figure (1): High level processes and information flows within a typical telecommunications service provider [2].



The **Billing Systems** is then responsible for using service usage data collected in CDRs to calculate call charges based on service rate plans and other customer service information. They may also produce billing information and bills to customers, process their payments and manage debt collection. In practice Telcos may have multiple billing systems and platforms to support different service revenue streams (e.g. consumer and business long distance voice, satellite TV, high speed internet, and business data services). In such a scenario a telco may implement an **Invoicing System** whose primary function is to aggregate billing data from multiple source billing systems to calculate any applicable service bundle and volume discounts, and produce consolidated customer invoicing.

Figure (2): Key OSS, BSS and revenue management system components, interfaces and high level information flows within a typical telecommunications service provider [2].

Telecommunications Service Provider (Telco) OSS, BSS and Revenue Management Systems



Information Security and Business Impacts

The use of Telco switches and related OSS and BSS systems have many benefits which include the ability to automate and accurately collect, store, process, use and analyze vast amount of CDR data in "real time" in many instances. However this is a double edged sword which presents certain risks to these assets, which include: the need to protect their physical and environmental security; availability; confidentiality and data integrity of their information. In addition, CDR data can be corrupted due to certain system conditions (e.g. interface failure and errors, corrupt files) and human user error. They may also be lost or corrupted due to natural and man-made calamities including intrusion, sabotage and manipulation by malicious entities or persons.

For example BCE Inc. reported $4,769 million in wireless service revenue and $3,755 million in wireline local, access and long distance revenues for 2011 [1, p44, p45]. These large revenue streams use CRDs as the basis for subscriber service billing calculations, invoicing and revenue collection. Therefore it is critical that telcos protect the confidentiality, integrity and availability of this information to ensure continuity of these revenue streams.

Group Project: Collecting Huge Amounts of User Data

BCE Inc. also reported that they had $15,390 million in network infrastructure and equipment as at the end of 2011, a significant portion of which represents Telco switching equipment, OSS, BSS and revenue management systems which generate and/or process CDRs [1, p99]. These assets represent the critical core of telco business operations without which they will be unable to provide services to their customers. Hence, it is clearly evident that there should be good policies in place which are adequately enforced to ensure the physical security, availability, and integrity of the information in the network assets and systems.

Telcos in Canada are regulated by the **Canadian Radio-television and Telecommunications Commission (CTRC)** which regulate telephony services in Canada and also stipulate certain mandatory safeguards and reporting requirements.

In addition Telcos in Canada also need to ensure they confirm to the **Personal Information Protection and Electronic Documents Act (PIPEDA)** relating to data privacy. This act is of particular relevance to information that is collected in a CDR as it is specifically identifiable to an individual person (for consumer subscriber services) and will be classified as "personal information" subject to confidentiality requirements.

In addition telecommunications infrastructure of a country is considered a critical strategic asset of the nation which requires a high level of protection from both external and internal saboteurs.

CONCLUSION: Key Security Policies for a Telecommunications Service Provider

Based on the above security and business impacts, the most important security policy areas for a telco relating to large data collection and processing functions are as follows:

1) **Physical and Environmental Security** related to Telco network equipment, operational support, business support and revenue management systems.
2) **Communications and Operations Management** related to IT data centres, network services and operations.
3) **Access Control** which protects the privacy, security and confidentiality of telco information assets by stipulating the rules for identification, authentication, authorization and acceptable use of systems by users (whether individuals or other systems).
4) Business Continuity Management.
5) Regulatory Compliance.

The remainder of the group project will focus on the critical **top three** ISO 17799 security domains and will present some key policies relating to these areas.

Group Project: Collecting Huge Amounts of User Data

Section: A	**TELCO Information Security Policy**	**Effective Date**: **Dec 4, 2012**
Statement of Authority	The Chief Information Security Officer has the authority to develop, implement and enforce IT Security Policy.	
Subsection : A1	**Physical and Environmental Security Policy**	**Change Control #: 1.4** **Author: Muath Al-Badawi**
Policy :	**Securing Telco Data Centre and Central Office Equipment**	**Approved By: Chief Information Security Officer**

Objective:	Define a secure and protected physical place where Telco confidential data will be hosted in.
Purpose:	The purpose of this policy is to protect the areas where critical Telco equipment, information assets and related confidential data are stored and processed.
Audience:	This policy applies to all Telco Data centres, Central offices and higher security zones.
Policy:	• Data centres and Central offices classified as a higher security zones. • Accessing Telco higher security zones shall be restricted to authorized employees only. Written authorization required for the other employees and has to be logged immediately. • Use a special badge colour for the authorized employees, where all other colours should be supervised whenever they are inside Telco higher security zones. • All access cards must be covered with a special plastic covers to be protected against copying and compromising. • No food and drinks are allowed. • Equipment especially telephone switches shall be housed in restricted areas with environmental controls; which include but not limited to temperature and humidity control. • Cell phones and any other non-Telco portable storage media are prohibited inside the data centre. • Unauthorized removal of Telco data, equipment and other related information systems resources is strictly prohibited. • All Telco higher security zones must conform to Telco physical security measures in order to provide secured and protected place.
Exception:	No exceptions for this policy.

Group Project: Collecting Huge Amounts of User Data

Section: A	**TELCO Information Security Policy**	**Effective Date: Dec 4, 2012**
Subsection : A2	**Physical and Environmental Security Policy**	**Change Control #: 1.2** **Author: Muath Al-Badawi**
Policy :	**Power Supply**	**Approved By: Chief Information Security Officer**

Objective:	To prevent or minimize network failure/unavailability and critical information system downtime caused by power outage.
Purpose:	The purpose of this policy is to protect Telco information assets and data processing from loss and damage as a result of unstable electrical supply.
Audience:	This policy applies to all Telco equipment, UPS devices and power generators.
Policy:	• UPS devices and power generators should be located in a higher security zone. • Instructions of use, manuals and technical support contact information shall be attached to the device itself. • UPS devices and power generators have to be maintained and tested on quarterly bases. • UPS devices and power generators maintenance and testing activities should be done within the maintenance window. All of these activities should be logged and dated. • Telco equipment with a dual power supply should be connected to two different electrical power substations. • Equipment with a dual power supply has to be checked for power supply failure every week. • All power connections, testing and maintenance should be done according to manufacturer's instructions by properly qualified and trained personnel. • Power off all equipment and personal computers that are not in use especially after working hours.
Exception:	No exceptions for this policy.

Group Project: Collecting Huge Amounts of User Data

Section: A	**TELCO Information Security Policy**	**Effective Date: Dec 4, 2012**
Subsection : A3	**Physical and Environmental Security Policy**	**Change Control #: 1.4** **Author: Muath Al-Badawi**
Policy :	**Secure Equipment Disposal**	**Approved By: Chief Information Security Officer**

Objective:	Provide a trusted mechanism to get rid of all unnecessary Telco equipment and materials.
Purpose:	The purpose of this policy is to prevent unauthorized access to confidential and sensitive Telco data stored in the unnecessary equipment and materials.
Audience:	This policy applies to all equipment that is no longer needed or corrupted.
Policy:	• Appropriate Approvals should be obtained prior to the destruction date. • Data custodians are responsible to get this approval from the authorized managers. • IT manager approval is a must for all special equipment. • Log all disposal activities and archive those logs. • All Telco equipment and assets that get approval for destruction should follow the equipment disposal standard. • All disposal procedures must be supervised by the operations team leader.
Exception:	Exception applies only for brand new unused equipment.
Physical and Environmental Policy Disciplinary Actions:	Any violation to the physical and environmental security policy will be considered a violation of the employee contractual agreement. Appropriate disciplinary action will apply and which may termination of employment for employees and termination of contracting agreements for contractors and consultants.

Group Project: Collecting Huge Amounts of User Data

Section: B	**TELCO Information Security Policy**	**Effective Date**: **Dec 4, 2012**
Subsection: B1	**Communications and Operations Management**	**Change Control #:** 1.0 **Author: Ben Yankson**
Policy:	**Backup and Restore Policy**	**Approved By: Chief Information Security Officer**
Objective:	To uphold the integrity and availability of information processing and storage devices essential for Telco business operations through standard processes setup for executing data and system state backup and providing timely restore. This is to allow critical data and systems essential to Telco operations be restored or recovered promptly in the event of data loss, corruption or systems malfunctions; and reduces the risk of Telco data in storage or transit being lost.	
Purpose:	To allow data and system essential to Telco operations to be recovered in a timely manner, based on the predetermined critical scheme, in the event of data loss or corruption within Telco Infrastructure.	
Audience:	Back-up Operators, Network Technicians, and Information owners.	
Policy:	• All Telco systems should have some sort of backup system. • All Telco systems including switches and servers should have some sort of failover functionality that is tested on a quarterly basis. Refer to SOP for setting up failover. • Regular backup of system state should be conducted anytime a change is made to server systems. All data should have weekly full backup on Fridays, and scheduled daily incremental backup Saturday to Thursday. • Two back-up copies of data should be kept at any given time. One copy on-site and the other at an offsite location, which is subject to the same environmental and physical protection policy established by the company, and data transferred through a VPN. • All back-ups will be verified by software on completion and an automatic failure or success log generated. Any back-up failure triggers an automatic email warning to all members of the Back-up team. • Regular testing and full restoration of backups to a separate system should be implemented and recovery test conducted once every six months. • Retention periods for backup information about Telco clients should be based on current Telco information retention plan; information owner of customer records must approve any destruction of client records. • Backup media should be appropriately disposed-off following. decommissioning procedure stipulated in the Telco Secure Equipment	

	Disposal Policy. • All Backup Operators at the company will be required to undergo backup process training, and awareness session for regulatory and legislative requirement personal data. • All data Restore requests will be submitted to Telco Computer Help Desk in written, with approved from Departmental Manager, which will then be forwarded to the appropriate System Manager responsible for the system on which the data was stored. Data should not be ever restored to a removable device. All data should be restored to the network drive.	
Exception:	System State data for individual employee computers are not required to be backed up, except when specifically deemed as required by appropriate management decision.	
Disciplinary Actions:	Any deviation from this policy could result in severe disciplinary action up to termination of employment with the company, and possible legal action.	
Section: B	**TELCO Information Security Policy**	**Effective Date: Dec 4, 2012**
Subsection: B2	**Communications and Operations Management**	**Change Control #: 1.0** **Author: Ben Yankson**
Policy:	**System and Network Data Protection Policy**	**Approved By: Chief Information Security Officer**
Objective:	To protect Telco devices and data from been compromised by external sources such as malware, or any unauthorized access by anyone outside the company.	
Purpose:	To protect the integrity and confidentiality of data within the company network infrastructure and computer systems.	
Audience:	All Network Services employees and computer system users.	
Policy:	• Wireless networks must enable encryption and apply controls to protect data passing over the network and prevent unauthorised access. • Disabling unnecessary services within Telco network that is not required to achieve Telco business functions; such as FTP server, and Telnet services. • All systems joining the company information systems network must have antivirus protection and automated installation of security patches enabled. • Network Operation should perform continuous vulnerability scans and automatically block all connected devices without recommend antivirus and operating system patches. Antivirus software is available to employees	

	through the company I.T Help Desk. • Telco systems and switches that support processing, storage, or transmission of confidential data must be monitored for intrusion with IDS/IPS technologies. Intrusions must be reported as per the Telco incident reporting policy. • Company devices signed out to employees must be password protected and automatic data encryption enabled to encrypt hard drive or any removable media attached. • All confidential email must be transmitted following company email transmission standards. For company email standard refer to "Email Use Standards" document.
Exception:	No Exception.
Disciplinary Actions:	Failure to adhere to this policy may result in severe consequence including but not limited to termination and possible legal action.

Group Project: Collecting Huge Amounts of User Data

Section: C	**Information Security Policy**	**Effective Date: Dec 4, 2012**
Subsection : C1	**Access Control Policy**	**Change Control #: 2.0** **Author: Cate Dillon**
Policy :	**User Access Management Policy**	**Approved By: Chief Information Security Officer**

Objective:	Define user access control measures for all systems and applications within Telco. This policy applies to all phases of the information lifecycle at Telco from its creation through access, use, maintenance, archives and destruction. It takes into account all forms of communication mechanism.
Purpose:	The purpose of this policy is to protect the privacy, security and confidentiality of all Telco information assets accessed through Telco or business partner systems.
Audience:	All employees and contractors of Telco.
Policy:	**Identification of Users and Systems** • Each user is assigned a single unique identifier. **Password** • Each user is provided confidential initial password that is system generated without human intervention valid for a limited period. • The systems should allow user to reset the passwords in a format as per *User Access Management Standards and Guidelines document*. • The password must be stored in a format that is not human readable and encrypted. • The management should periodically review the encryption method to ensure that it maintains systems privacy, security and confidentiality. **Authentication** • The authentication is granted to each system and application only on presenting unique identifier and a valid password. • Authentication credentials should not be hard coded within the system or applications when accessed by individual user. The credentials should be encrypted and separated from the code when accessed by system. **Authorization** • The access should be granted based on least privilege principles and access requests should be formally made and approved by the system/application owner or an authorized delegate. • All accesses to the system should be logged and maintained for period as per *User Access Management Standards and Guidelines document*. • The privileges granted should be reviewed in the event of every job description and organizational structure changes. • All access of a user exiting employment or contract must be deleted

	immediately prior to the closing day of employment. **Acceptable Use of Systems** • The authentication credentials and privileges are assigned to a specific user for carrying out his/her roles and responsibilities. Under no circumstances is a user to give, tell or hint at their password to another person including IT staff, administrators, superiors, other co-workers, friends and family members either verbally or electronically such as email or internet social media sites. • If an employee either knows or suspects that his/her password has been compromised, it must be reported to the Information Services and the password changed immediately. **Management Responsibility** • Establish appropriate procedures and standards to determine clear ownership of data and system, access change management, least access privilege rules and information classification structure. • Provide on-going education to ensure users are provided with communication, supporting tools and training as appropriate to enable them to fulfill their duties as they relate to protection of information. **Data and System Owner Responsibility** • Must have documented procedures to control access to the information and system. • Provide logs and records identifying access requests approval for audit purposes. **User Responsibility** • Promptly report any incidents that have a potential security impact to ABC Telco (commonly referred as 'Telco') to the Information Services.
Exception	• In case of Telco user accessing business partner system, the password granted may follow the standards set by the business partner. • Any departure from this policy should be approved by Chief Information Security Officer, documented and retained for audit purposes.
Enforcement	Any individual user of the system found to be non-compliant with this policy will be met by disciplinary action which may include termination of employment or contract.

Physical and Environmental Security Policy Standards

Version: 3.0
Approved by: Chief Information Security Officer
Date: Dec 4, 2012

Physical security measures:

- All new and existing data centres should be located in areas unlikely to experience natural disasters.
- Should be protected against fire, water damage, vandalism, and other threats.
- No windows allowed and all entrances shall be monitored from both sides (internal and external).
- All entrances shall be provided with access door mechanism. Entrance doors should be closed automatically after they have been opened and should set off the alarm if they remain open for a certain amount of time.
- Man trap access should be used and maintained on a yearly basis.
- All walls and openings to Telco data centres should be resistance to fire and forcible entry.
- Monitoring system, all fire alarms, motion, carbon dioxide, water and other detectors shall be tested and maintained on a monthly basis.

Equipment disposal standard:

- Data storage media should go through two stages of disposal, the first one is to apply metal pin destruction then should be sent to drive shredder machine.
- All other devices should be clear of any storage media before applying the disposal mechanism that send them to the metal shredder and then to be recycled.

Group Project: Collecting Huge Amounts of User Data

Email Use Standards
Version: 2.0
Approved by: Chief Information Security Officer
Date: Dec 4, 2012

All company employees must be careful when sending email containing confidential data as e-mails sent over public network susceptible to interception, and can result to breach on confidentiality. All employees are required to abide by the following email transmission rules.

- Confidential emails must be addressed to recipient with legitimate authorization (clearance).
- Senders should verify the **send-to email address** before sending messages containing confidential data.
- All employees should have an appended e-mail signature requesting unintended recipient of emails to discard emails immediately.
- The confidential content of the email should be kept at minimum to achieve the intended purpose of the message.
- Senders should use encrypted email services wherever such services are available
- Users should use secure file transfer services when sending large confidential files outside the organization with different encryption scheme.

Group Project: Collecting Huge Amounts of User Data

User Access Management Standards and Guidelines
Version: 2.0
Approved by: Chief Information Security Officer
Date: Dec 4, 2012

Passwords:

- The passwords have a minimum length of 8 alphanumeric characters and must include combination of both alphabetic characters and numeric digits. It should contain at least one special character (e.g. @, %, $, #, !, etc.).
- The password must not be same as any of the previous 4 passwords.
- The password expires every 90 days or less.
- The user access is lockout after 5 unsuccessful login attempts.
- Any locked account requires Administrator intervention in order to unlock it.
- The users must be positively identified prior to obtaining a new or changed password.
- Passwords must be encrypted immediately after being entered and decrypted at the last stage of the authentication process.
- Passwords must only be deciphered during the login process and against the identity given.
- Cookies used to manage state must be encrypted and deleted at the end of the session
- Cookies must not be used to store passwords.
- All software and files containing formulas, algorithms and other specifics of the process used to generate passwords must only be accessible by processes not individuals.
- On Automatic password reset completion, the system should inform the user by an alternate channel of the event occurrence.

Guiding Principles

- Protect the safety and respect the confidentiality of information through appropriate safeguards.
- Make reasonable efforts to ensure information is accurate, complete and relevant.
- Limit release, access and use of information to what is necessary to perform a task.

Security Policies & Risk Mgmt (MITS 5600G)

Group Project: Collecting Huge Amounts of User Data

Definitions:

Access: An ability to use or modify data or system.

Access Control: The measures to grant or deny an access to the user.

Business Support Systems (BSS): Business Support Systems (BSS) includes applications which support revenue management, order entry, customer account management and product management within a telecommunication company.

Call Detail Record (CDR): A Call Detail Record is created by a telephone switch that records detailed information about telephone calls placed by subscribers and users of the telecommunications facility and further processed by Operational Support Systems (OSS) and Revenue Management Systems. In a telephone switch, a CDR contains information about all the calls passing through the telephone exchange. The CDRs are generated by Automatic Message Accounting (AMA) and further processed by Operations Support System (OSS) and Revenue Systems.
A fully processed subscriber CDR for long distance voice calls will contain information about recent system usage such as the identities of call origin, identities of destinations call endpoints, duration of each call, and the amount billed for each call. They may also include other details such as the total usage time in the current billing period, total free time remaining in the billing period, and the running total charged during the billing period. The format of the CDR varies among different Telco providers and by service types.

Central office: Is the place where the critical Telco equipment is housed, for example: telephone switches and interconnects devices.

Data centre: Is the facility that host Telco computer systems, servers, network and all sensitive devices that are necessary for Telco business continuity.

Data custodians: is the IT employee who has administrative control and responsible for protecting Telco data and information assets.

Higher security zones: All rooms that holding sensitive data processing and sensitive equipment such as data centres and central offices.

Information Asset: A definable piece of information, stored in any manner that has a recognized value.

Least Privilege Principle: Access privileges granted to a user to complete duties assigned and nothing more.

Maintenance window: Is a regular window of time scheduled and approved by IT management to do all maintenance work related to higher security zones while minimizing unavailability of information systems and services to the customers.

Group Project: Collecting Huge Amounts of User Data

Man Trap access: two levels of access doors works the same way if you are getting in or out where the second door does not open before closing the first one.

Metal pin destruction: destroying mechanism applied by pressing down metal pin on the hard drives.

Operational Support Systems (OSS): OSS are computer systems used by telecommunications service providers which most frequently describes network systems dealing with the telecom network itself, supporting processes such as maintaining network inventory, provisioning services, configuring network components, and managing faults. In general OSS covers the following process and application areas: network management, service delivery, service fulfillment including network inventory, activation and service Provisioning, service assurance and customer care.

Special equipment: Equipment housed on the higher security zones that have sensitive information such as storage devices, Servers, telephone switches and network appliance.

Telco Billing System: Telecommunications billing system is an enterprise application software designed to support the telecommunications billing processes. They are responsible for using service usage data collected in CDRs to calculate call charges based on service rate plans. They may also produce billing information and bills to customers, process their payments and manage debt collection.

Telecommunications: Telecommunications means communication by electrical or electromagnetic means, usually (but not necessarily) over a distance utilizing wire, optical fiber, radio waves or other electromagnetic systems.

Telecommunication Switch: A telephone switch is a system of electronic components that connects telephone calls. Telco switches are housed in a Central Office (CO) which is a physical building which includes inside plant equipment and telephone switches, which make telephone calls by making connections and relaying the speech information.

UPS: Uninterruptible Power Supply.

User: Individual or System.

References:

[1] Bell Canada Enterprises (BCE) Inc. 2011 Annual Report, http://www.bce.ca/assets/Uploads/Documents/archivesAnnualReport/BCE/2011/BCEAR2011EN.pdf (accessed 27 November, 2012).

[2] D. Devendra, Thejes Consultancy: Sample Telco Process Design, http://www.thejes.com/development1/index.php?option=com_content&view=article&id=102&Itemid=176, (accessed 27 November, 2012).

[3] S. Rowe II, Telecommunications for Managers, Prentice-Hall, Englewood Cliffs, 1995

[4] S. Greene, Security Policies and Procedures: Principles and Practices, Pearson Prentice Hall, 2006