Drill Here

Emerging MSO Technology: Systemic Prioritization of Undetected Service Outages to Improve Overall Business Performance

A White Paper Prepared for the
Society of Cable Telecommunications Engineers

By Robert F. Cruickshank III
Chief Technology Officer, Rev2

Abstract

While cable television Multiple System Operators (Cable MSOs) have alerting mechanisms and are equipped to deal with “right now, hard down” critical outages, oftentimes smaller and intermittent outages are much harder to detect and can be altogether missed for extended periods of time. But customers notice these intermittent outages – especially business customers – and some of these intermittent outages are the precursors of much larger outages. The good news is there are clues that can clearly point operations teams to concentrations of outage risk. The bad news is these clues are too often imprisoned in disparate databases. A solution is found by carefully classifying, scoring and combining maintenance activities, telephone calls from troubled subscribers, truck rolls and network telemetry – resulting in timely identification of otherwise undetected outages.

Introduction

Service reliability is increasingly important, especially for business customers. In the quest for 99.999% service availability – or 5.3 minutes per year maximum downtime per customer – Cable MSOs have dedicated teams searching for subscriber outages. When these teams are provided with an automated aggregate view of outage risk, they spend less time marshaling data between databases and spreadsheets, and more time on geographically targeted analysis, maintenance and repairs.

Mathematically, risk is defined as [the probability of an outage] times [the expected loss associated with the outage]. When there are multiple potential outages and different costs associated with them, the formula becomes:

$$\text{Risk} = \sum_{i}^{\text{outages}} [\text{probability of } ith \text{ outage}] \times [\text{cost of } ith \text{ outage}]$$

Business customers and triple play customers, which generate much higher revenues than basic cable customers for MSOs, also have a much higher cost associated with each outage. The loss of that customer due to too many intermittent outages is a bigger hit to long-term revenue. As a result, with aggregate outage risk concentrations clearly portrayed and delivered to the proper audiences, Cable MSOs are able to find and fix the most critical outages as soon as possible and can also fix more outages faster, reduce costly phone calls and truck rolls, reduce subscriber churn (especially from high-revenue customers) and improve overall service reliability.

Measured Business Value

The risk concentration analysis solution has proven capable of providing a straightforward return on its value to MSOs. On average, MSOs expect at least a 1.5% reduction in technical calls per month and an associated 1.5% reduction in truck rolls related to trouble calls per month. For an MSO with 1 million subscribers, that represents a reduction of approximately 5,000 calls per month and 1,000 truck rolls per month. After deploying the solution, one of the world’s largest MSOs projected an overall Net Present Value of $1.2m – a payback of less than two years. The NPV included measurable before and after savings attributed to preventing thousands of phone calls, truck rolls, ticket handoffs, repeat tickets and customer credits, and close to 2 million preventable subscriber outage minutes.

Increased operational efficiency provides measurable value as well. Another of the world’s largest MSOs anticipated the following annual returns on personnel investments based on the increased efficiency of its operations staff:

- $1m/year (or 100% ROI) based on a 50% reduction in the time for the network QA team to identify undetected infrastructure problems;
- $.3m/year (or 30% ROI) based on time freed up for the network QA team to make additional analyses;
- $2m/year (or 200% ROI) based on extending the capabilities of the engineering team;
- $4.2m/year (or 11% ROI) based on an increased ability to optimize spending, such as identifying recoverable spending opportunities, identifying high value investment opportunities, and avoiding operations costs.

Background & Opportunity

Cable MSOs generally detect outages in node-serving areas by looking for subscriber trouble call volume at or above a threshold of approximately three calls per hour. Yet there are few automated solutions for automatically processing low-level “dribbling in” trouble calls and truck rolls over several days or weeks. Likewise, while detection exists for multiple Customer Premises Equipment (CPE) devices falling offline (i.e. number of offline devices rising above a certain threshold), there are few automated solutions for smaller deviations in offline devices, and worse yet insufficient linkages and ties among disparate database records of subscriber calls, truck rolls, and offline devices.

A challenge Cable MSOs often face is the “silo” nature of operations databases that store outage risk data. There is often one database that contains troubleshooting records from voice and data subscribers; a second database with troubleshooting records from video subscribers; a third database with truck rolls to subscribers; a fourth database with physical plant maintenance truck rolls; a fifth database with network telemetry readings, etc. Generally, these databases are dissimilar enough that aggregate analysis of their data is time consuming and tedious.

Due to the aforementioned challenges, smaller outages and pockets of degraded service may go undetected long enough for repeat calls to manifest as complaints to Cable MSO executive management – often resulting in staff ultimately finding and validating an actual subscriber-affecting issue and then regretfully agreeing “Why didn’t we see that earlier?”

Similarly, risk concentration analysis aids in the ability to separate real detections from false alarms (i.e., Type I and Type II errors). A typical MSO generates so many alarms that engineers tend to ignore them. By correlating, classifying and aggregating micro alarms, the MSO is provided with a very high probability of detection and a very low false alarm rate, alleviating a major drawback of current alarm technology.

Methodology

Multiple records are used to point to material concentrations of risk. A critical advantage of the risk concentration analysis methodology is classifying risk data in a meaningful way so that Cable MSOs can see these concentrations. These “risks that matter” become evident when each risk is considered in the context of all other risks existing throughout the service delivery and support infrastructure. The methodology addresses the reality that different risks have different impacts on the business. The primary differentiator is determining where there are concentrations of risk. With risk concentration analysis, material risks emerge when correlating risks from all silos and considering each risk in context of impact to the business. This approach yields Financial and Reputational scores, making it easy to recognize and prioritize material risks.

This is accomplished by collecting all risk data from across the Cable MSO's business and service delivery infrastructure, and then normalizing risks into a common format and language so they can be compared by assigning a unique Financial and Reputational score to each risk.

The score of each risk reflects its materiality to the business or subscriber – as well as the impact that problem would cause. When visualized, the risks that represent the greatest vulnerabilities will stand out from the rest. This helps Cable MSOs identify risks and then test controls in the context of all other risks, as opposed to looking at risks in isolation. This identifies, for example:

- Chronically misbehaving devices;
- Recurring problems specific to a geographic region or departmental silo;
- Problems in program execution that are impacting the business's reputation or financial bottom line – and could escalate.

Required elements include a highly extensible "cache and store" risk data warehouse, data source adapters, data I/O, analytics, a visualization tool and web services interfaces as shown in Figure 1.

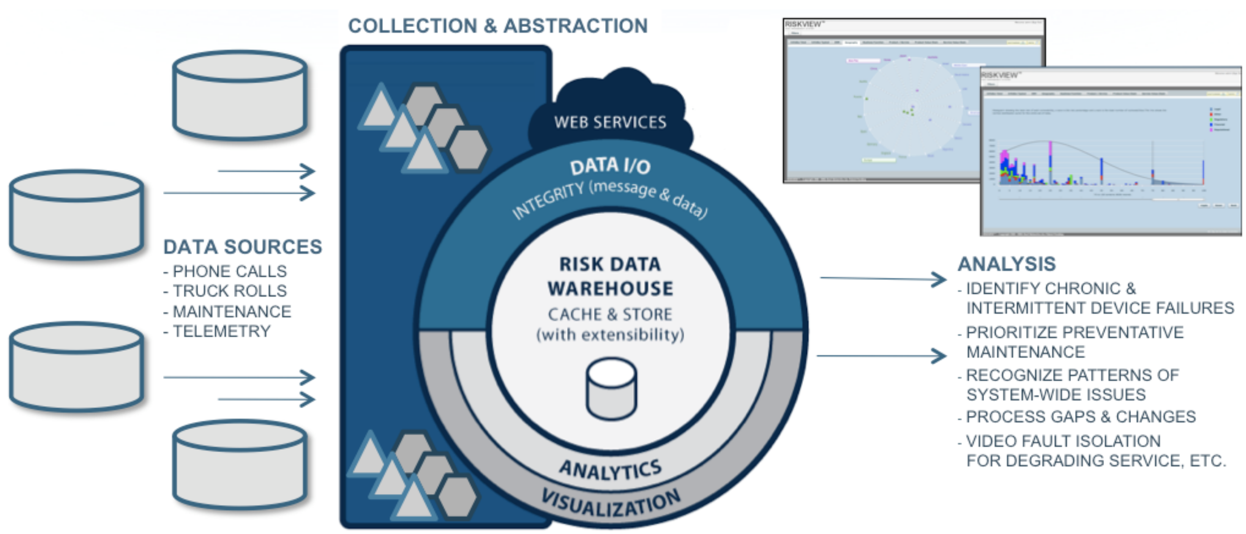

Figure 1. Risk Concentration Analysis Management Architecture

Examples of data sources in Figure 1 include telemetry data, troubleshooting records from voice, data and video subscribers, subscriber truck rolls, and physical plant maintenance truck rolls.

In summary, risks are analyzed in the context of all other risks because isolated risk analysis doesn't provide an efficient way of looking at the larger picture. While isolated risk analysis evaluates each standalone tree, it ignores the much larger level of the forest. Additionally, isolated analysis lacks consistency and the ability to assign relative weights to risks, making it hard to compare risks from seemingly unrelated areas.

The Role of Enhanced Telemetry

Another insightful source of information is telemetry data from in-home and in-business CPE devices such as cable modems and set-top boxes that support the DOCSIS (Data Over Cable Service Interface Specification). In concert with network elements such as cable modem termination systems, DOCSIS devices provide remote access to several metrics such as Uncorrectable Error Rates (UER), elevated reset behavior, and unusual online/offline behavior – on both the shared downstream and upstream channels as well as to and from each individual device. Even more insightful, depending on the frequency and magnitude of DOCSIS telemetry readings, the level of subscriber pain can vary. Examples include:

- A cable modem that spontaneously resets once a week is less of a problem for a subscriber than a modem that resets tens or hundreds of times per day.
- A cable modem with -9 dBmV downstream receive power is less problematic on hot summer days than a modem with -9 dBmV upstream receive power.
- A cable modem or set of cable modems with high Uncorrectable Errors is more problematic than a similar set of modems with high Correctable Errors. But these are of greater concern than a set of modems with very low numbers of Correctable Errors.

An important requirement is uniquely classifying and scoring DOCSIS CPE telemetry data so that <u>those specific telemetry readings having greater impact to subscribers are given greater importance</u> and higher Reputational cost scoring. By doing so, an aggregate tonnage of risk concentration can be easily calculated and then used to prioritize maintenance and repair efforts.

Case Study: Correlation of Subscriber Call Volume with DOCSIS Telemetry

Recent efforts have shown direct correlation between DOCSIS telemetry and the likelihood of troubled subscriber phone calls and truck rolls. In brief, when telemetry indicates a problem, subscribers are unhappy and ultimately call for help, which drives costs.

In order to confirm the longstanding belief that subscriber-affecting network issues could have been detected earlier, the following plan was put in place at a North American Cable MSO:

1. Identify Persistent Worst Nodes by “Connectivity” Call Volume only for those serving areas where a Network Outage had not been declared in a135-day period.

2. Tally the following “Connectivity” call types (per node total calls and average calls shown):

   a. Internet – Loss of Connection: 50 Calls, 0.37 Calls per day,

   a. Internet – No Connection, Signal Related: 34 Calls, 0.25 Calls per day,

   b. Internet – Slow Speeds: 4 Calls, 0.03 Calls per day,

   c. Voice – Loss of Dial Tone: 66 Calls, 0.49 Calls per day,

   d. Voice – Intermittent Loss of Dial Tone: 48 Calls, 0.36 Calls per day,

   e. Voice – Quality of Service (Voice Quality) Issue: 13 Calls, 0.10 Calls per day.

2. Plot Call volume and the following DOCSIS Telemetry Metrics by day over time:

   a. Uncorrectable Codeword Error Rate (CER as Shown in Figure 2),

   b. Elevated Reset behavior, and

   c. Online/Offline behavior.

A leading MSO was experiencing a fluctuation in call volume correlating to Uncorrectable Codeword Error Rate (CER). Similar correlation was found across all nodes among DOCSIS metrics for CER, elevated device resets and time-varying online/offline status. Surprisingly, the worst node for slow speed call volume correlated not with traffic, but with Uncorrectable Error Rates!

If not for the correlation study, the lingering issue might have continued undetected for much longer. With the study it was fixed with pro-active maintenance activity, but only after affecting subscribers for three months over which the MSO received 108 “Connectivity” phone calls, performed 12 plant visits, and 48 premises visits at a total cost of approximately $7,000 plus subscriber churn.

Return on Investment Analysis

In the systemic treatment of undetected outages, value is realized in each of the following three areas:

1. Groups that perform outage detection and analysis:

    a. These groups are tasked with finding outages, and answering the question “why did a certain event occur for a significant amount of time without an outage ever being declared?” These groups are then tasked with creating new queries to automatically declare outages (i.e. pull the fire alarm) usually after an irate subscriber phones/emails, the CEO, or a financial analyst notices an unusual spike in truck rolls in a specific region or an abnormally high percentage of calls related to a specific product. Without the benefit of Risk Concentration Analysis, this process often takes weeks or months of sifting through data and building Microsoft Excel macros, sorting filters and spreadsheets.

    b. Reducing the time to resolve and understand causes of issues to 25% of the typical time required increases the value of these groups by a factor of 4x.

2. Engineering, customer service and network operations:

    a. Engineering, customer care and network operations organizations are constantly asked to resolve issues due to failed architectures, equipment or applications.

    b. Better understanding subscriber-affecting problems extends the capabilities of these organizations by an additional 75%.

3. Enterprise:

    a. Ability to optimize spend to the areas that impact the most subscribers vs. “one-offs or squeaky wheels” significantly improves the customer experience and improves overall operational efficiencies of the MSO. The continued positive impact of fact-based decision-making on enhancements and new initiatives pays dividends for years into the future.

Anticipated Form of Final Results

Depending on user needs and type of outage investigation, and because certain outage types are easier to detect than never-before-seen outages, flexibility is required so that results may be grouped and viewed in different ways. In all views the net outcome is a specific recommendation to “Drill Here,” meaning Operations should have a closer look specifically at one of more of the following:

- Geographical Area: Market, Hub, Node, Last Active Amplifier or Street;
- Customer Premise Equipment: Make/Model/Hardware/Firmware/Software;
- “Mother Ship” Network Element: CMTS, DNCS, DHCP Server, DNS Server, Soft Switch, etc.;
- Product or Service: Voice, Voice Mail; Video, VOD; Data, etc.

Because of the aforementioned need for flexibility, outage data may be viewed in at least three ways. First, a user interface allows for exploratory data mining and is best for analysis. Figure 2A is a view of all the hubs in a Cable MSO. Each dot on the radar chart represents the “Aggregate Financial Outage Risk” or “Aggregate Reputational Outage Risk” normalized for the number of Revenue Generating Units (RGUs) per hub. Distance from center indicates badness, worst at edge. In Figure 2A, there are many hubs portrayed, but only a few outliers. Note how the top three to five outliers clearly distinguish themselves further from the center than the rest.

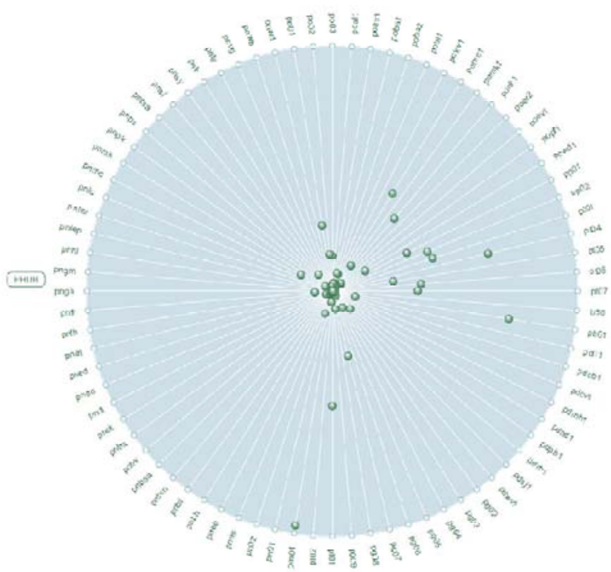

Figure 1A. The Interactive User Interface View of Hubs

Figure 2B is a view of all the nodes in the worst hub (pm01) shown in Figure 2A. In Figure 2B there are hundreds of nodes portrayed. Note again how the top outliers – the worst nodes in the worst hub – clearly stand out. In both figures, each dot represents the aggregate normalized Financial or Reputational outage risk cost.

Figure 2B. The Interactive User Interface View of Nodes in Worst Hub

The second way to view Outage Risk is by means of reports that are most useful when insights from exploratory analysis in the user Interface have made the outage easy to find systemically. Reports can be constructed for specific audiences of fix agents and locations such as the “Department Head of Field Service in Syracuse.” Reports can be run on-demand or on a periodic basis every Day, Week, Month, Quarter, or Year. Reports may be automatically emailed and are easily viewed in Microsoft Excel.

Reports are extremely flexible and can be configured to effortlessly identify, for example, the Top 10 Worst Markets, Hubs, Nodes, Last Active Amplifiers, and Streets, either system-wide or by specific Management Area(s). Any number of Classifications may be used: by Asset, by Product, by Trouble Type, by Fix Activity, and as always include both Reputational and Financial scoring. The sample report in Figure 3 is from the Top 2 Worst Nodes in an Entire Cable System and includes:

- Troubled Subscriber Phone Calls and Truck Rolls in Red,
- Telemetry Data from MAC Addresses in White,
- Plant Maintenance Truck Rolls in Yellow.

Notice the far right columns with Financial and Reputational (Outage) Costs. Observe that in Node 129174 phone calls and truck rolls dominated failed telemetry readings, and in Node 152280 failed telemetry readings dominated phone calls and truck rolls. Nodes can score badly for any number of reasons and worst performers rise to the top.

Count	VulnerabilityId	Date	ImpactCostType	Node	CompletionComments	Resolution	Up Rx	Up SNR	Up Tx	Dn Rx	Dn SNR	Product	CostFinancial	Calls	PctOutageCost
15	-	-	-	-	-	-						-	$ 1,114.07	4	0.27189
-	[illegible]	1/31/2011 16:26	Financial	129174	Cx Physical Reset	-	0	0	0	0	0	Phone	$ 8.86	1	0.00216
-	[illegible]	2/1/2011 0:00	Reputational	129174	-	-	2	29	53	-6	32	Internet	$ -	0	0.00002
-	[illegible]	2/1/2011 10:19	Financial	129174	Fault not Found	Follow Up Required	0	0	0	0	0	Internet	$ 9.06	1	0.00221
-	[illegible]	2/1/2011 10:20	Financial	129174	Provide information	Educated Cx	0	0	0	0	0	Internet	$ 9.06	1	0.00221
-	[illegible]	2/1/2011 10:24	Financial	129174	Fault not Found	Follow Up Required	0	0	0	0	0	Internet	$ 9.06	1	0.00221
-	[illegible]	2/2/2011 0:00	Reputational	129174	-	-	0	26	55	-7	37	Internet	$ -	0	0.00002
-	[illegible]	2/3/2011 0:00	Reputational	129174	-	-	1	30	43	0	0	Internet	$ -	0	0.00002
-	[illegible]	2/3/2011 0:00	Reputational	129174	-	-	0	26	55	-7	37	Internet	$ -	0	0.00002
-	[illegible]	2/3/2011 14:52	Financial	129174	TIGHTENED VSF^S AT PANEL. I	Tightened Equipment	0	0	0	0	0	-	$ 938.53	0	0.22891
-	[illegible]	2/4/2011 0:00	Reputational	129174	-	-	1	32	41	0	0	Internet	$ -	0	0.00002
-	[illegible]	2/4/2011 0:00	Reputational	129174	-	-	0	26	55	-6	37	Internet	$ -	0	0.00002
-	[illegible]	2/4/2011 9:38	Financial	129174	ELECTRICAL NOISE NOT FROM	Assisted Another Technician	0	0	0	0	0	-	$ 46.50	0	0.01134
-	[illegible]	2/4/2011 14:26	Financial	129174	FILTER^D ANOLGUE FEED TO N	Installed Noise Filter	0	0	0	0	0	-	$ 46.50	0	0.01134
-	[illegible]	2/4/2011 14:26	Financial	129174	NOISE ON ANALOG TV RISER, I	Installed Noise Filter	0	0	0	0	0	-	$ 46.50	0	0.01134
-	[illegible]	2/5/2011 0:00	Reputational	129174	-	-	0	29	54	-6	37	Internet	$ -	0	0.00002
48		-	-	-	-	-	38	1071	1387	26	1167	-	$ 1,247.38	4	0.30527
-	[illegible]	1/30/2011 0:00	Reputational	152280	-	-	1	27	40	-10	36	Internet	$ -	0	0.00002
-	[illegible]	1/30/2011 0:00	Reputational	152280	-	-	1	26	36	-17	31	Internet	$ -	0	0.00002
-	[illegible]	1/30/2011 0:00	Reputational	152280	-	-	1	23	38	5	39	Internet	$ -	0	0.00002
-	[illegible]	1/30/2011 0:00	Reputational	152280	-	-	1	23	39	10	36	Internet	$ -	0	0.00002
-	[illegible]	1/31/2011 0:00	Financial	152280	T=12/18/22, C=8/10/12, SWAP	DSTB Replaced - Defective	0	0	0	0	0	Digital	$ 58.02	1	0.01415
-	[illegible]	1/31/2011 0:00	Reputational	152280	-	-	1	23	49	3	39	Internet	$ -	0	0.00002
-	[illegible]	1/31/2011 0:00	Reputational	152280	-	-	0	23	39	3	40	Internet	$ -	0	0.00002
-	[illegible]	1/31/2011 0:00	Reputational	152280	-	-	1	25	36	-16	32	Internet	$ -	0	0.00002
-	[illegible]	1/31/2011 0:00	Reputational	152280	-	-	1	24	39	5	39	Internet	$ -	0	0.00002
-	[illegible]	1/31/2011 0:00	Reputational	152280	-	-	1	24	39	10	37	Internet	$ -	0	0.00002
-	[illegible]	2/1/2011 0:00	Reputational	152280	-	-	1	28	36	2	0	Internet	$ -	0	0.00002
-	[illegible]	2/1/2011 0:00	Reputational	152280	-	-	1	25	36	-17	32	Internet	$ -	0	0.00002
-	[illegible]	2/1/2011 0:00	Reputational	152280	-	-	1	23	43	4	38	Internet	$ -	0	0.00002
-	[illegible]	2/1/2011 0:00	Reputational	152280	-	-	1	24	39	10	38	Internet	$ -	0	0.00002
-	[illegible]	2/1/2011 11:45	Financial	152280	front aerial. incomplete, snow	Cable Located	0	0	0	0	0	-	$ 1,116.00	0	0.27220
-	[illegible]	2/1/2011 21:54	Financial	152280	Reboot Box	Resolved Issue	0	0	0	0	0	Digital	$ 6.28	1	0.00153
-	[illegible]	2/2/2011 0:00	Financial	152280	SPLITTER@TAP, WALL PLATE F.	Drop Fault Repair	0	0	0	0	0	Phone	$ 58.02	1	0.01415
-	[illegible]	2/2/2011 0:00	Reputational	152280	-	-	0	21	32	9	39	Internet	$ -	0	0.00002
-	[illegible]	2/2/2011 0:00	Reputational	152280	-	-	1	24	46	-3	39	Internet	$ -	0	0.00002
-	[illegible]	2/2/2011 0:00	Reputational	152280	-	-	1	25	36	-17	32	Internet	$ -	0	0.00002
-	[illegible]	2/2/2011 0:00	Reputational	152280	-	-	1	24	39	10	37	Internet	$ -	0	0.00002
-	[illegible]	2/2/2011 0:00	Reputational	152280	-	-	1	24	39	0	35	Internet	$ -	0	0.00002
-	[illegible]	2/2/2011 14:52	Financial	152280	Reset/reboot device	Resolved Issue	0	0	0	0	0	Internet	$ 9.06	1	0.00221
-	[illegible]	2/3/2011 0:00	Reputational	152280	-	-	0	22	0	9	0	Internet	$ -	0	0.00002
-	[illegible]	2/3/2011 0:00	Reputational	152280	-	-	1	28	0	1	0	Internet	$ -	0	0.00002
-	[illegible]	2/3/2011 0:00	Reputational	152280	-	-	1	27	0	12	0	Internet	$ -	0	0.00002
-	[illegible]	2/3/2011 0:00	Reputational	152280	-	-	1	25	36	-16	32	Internet	$ -	0	0.00002
-	[illegible]	2/3/2011 0:00	Reputational	152280	-	-	1	27	29	0	0	Internet	$ -	0	0.00002
-	[illegible]	2/3/2011 0:00	Reputational	152280	-	-	1	23	44	5	38	Internet	$ -	0	0.00002
-	[illegible]	2/3/2011 0:00	Reputational	152280	-	-	1	24	39	10	37	Internet	$ -	0	0.00002
-	[illegible]	2/3/2011 0:00	Reputational	152280	-	-	1	29	0	2	0	Internet	$ -	0	0.00002
-	[illegible]	2/4/2011 0:00	Reputational	152280	-	-	1	28	31	8	0	Internet	$ -	0	0.00002
-	[illegible]	2/4/2011 0:00	Reputational	152280	-	-	1	29	0	0	0	Internet	$ -	0	0.00002
-	[illegible]	2/4/2011 0:00	Reputational	152280	-	-	1	28	0	-3	0	Internet	$ -	0	0.00002
-	[illegible]	2/4/2011 0:00	Reputational	152280	-	-	1	28	0	8	0	Internet	$ -	0	0.00002
-	[illegible]	2/4/2011 0:00	Reputational	152280	-	-	1	23	39	3	39	Internet	$ -	0	0.00002
-	[illegible]	2/4/2011 0:00	Reputational	152280	-	-	1	25	36	-17	32	Internet	$ -	0	0.00002
-	[illegible]	2/4/2011 0:00	Reputational	152280	-	-	1	23	41	4	39	Internet	$ -	0	0.00002
-	[illegible]	2/4/2011 0:00	Reputational	152280	-	-	1	24	39	10	37	Internet	$ -	0	0.00002
-	[illegible]	2/5/2011 0:00	Reputational	152280	-	-	1	27	41	-10	36	Internet	$ -	0	0.00002
-	[illegible]	2/5/2011 0:00	Reputational	152280	-	-	1	22	41	9	39	Internet	$ -	0	0.00002
-	[illegible]	2/5/2011 0:00	Reputational	152280	-	-	1	24	39	9	37	Internet	$ -	0	0.00002
-	[illegible]	2/6/2011 0:00	Reputational	152280	-	-	0	27	43	-10	36	Internet	$ -	0	0.00002
-	[illegible]	2/6/2011 0:00	Reputational	152280	-	-	1	22	41	8	39	Internet	$ -	0	0.00002
-	[illegible]	2/6/2011 0:00	Reputational	152280	-	-	0	23	40	2	39	Internet	$ -	0	0.00002
-	[illegible]	2/6/2011 0:00	Reputational	152280	-	-	1	28	32	0	0	Internet	$ -	0	0.00002
-	[illegible]	2/6/2011 0:00	Reputational	152280	-	-	1	25	36	-18	31	Internet	$ -	0	0.00002
-	[illegible]	2/6/2011 0:00	Reputational	152280	-	-	1	24	39	9	37	Internet	$ -	0	0.00002

Figure 3. Output from Scheduled Report Emailed to Field Service

The third way to view Outage Risk is by auto-alarm generation and email distribution. Alarms can have the same look and feel as reports and are based on specific queries that, if any results are returned, send a clear message: mobilize now!

Conclusions

By using a framework and visualization engine based on next-generation data aggregation and correlation, Cable MSOs can identify chronically failing equipment, prioritize preventative maintenance, and find and prevent outages. Cable MSOs are able find outages that are otherwise “under the radar” and hurting subscribers.

Systemic treatment identifies how outage risks map together. Analyzing both outage events and associated network health telemetry metrics quickly isolates specific drivers of material outage – the outages that matter. This helps Cable MSOs recognize patterns of system-wide issues in the service delivery infrastructure, and reduce truck rolls and repeat service calls.

Suggestions for Future Work

- Further quantify the ROI benefit of systemic treatment of undetected outages in complementing existing MSO operational “right now” outage detection;

- Propose solutions for aggregating and processing “No Trouble Found” data;
- Further development of systemic filters to identify, classify and score both impact and non-impact failures (i.e., those that do/do not have material impact on subscribers), to further prioritize those failures that impact the delivery of services;
- Develop a sophisticated mapping system that enables the pinpointing of trouble-areas according to a visualization of their precise geographical location, down to the street level.

Glossary

CC – Call Center
A centralized office operated by a cable company to administer telephone-based support and information inquiries from subscribers.

CER – Codeword Error Rate
A technique that enables reliable delivery of digital data. Many communication channels are subject to channel noise so errors may be introduced during transmission from the source to a receiver.

Cloud
A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services). The idea behind the cloud is that it can be rapidly provisioned and released with minimal management effort or service provider interaction.

CPE – Customer Premises Equipment
Refers to equipment located at a subscriber’s premises and connected with a carrier’s telecommunications channels. Generally includes devices such as telephones, routers, switches, set-top boxes, fixed mobile convergence products, home networking adapters and Internet gateways that enable subscriber’s access to services from the home.

DOCSIS – Data Over Cable Service Internet Specification
An international telecommunications standard that permits the addition of high-speed data transfer to an existing CATV system. It is employed by many Cable MSOs to provide Internet access over their existing infrastructure.

Financial Risk
An umbrella term for any risk associated with any form of financing. Risk is often taken as downside risk, the difference between the actual return and the expected return (when the actual return is less) or the uncertainty of that return. In the Cable MSO world, financial risk is calculated using metrics such as truck rolls, call center calls, and churn rate.

MSO – Multi-System Operator
An operator of multiple CATV systems. In the strictest definition, any cable company that serves multiple communities is an MSO, however the term today is usually reserved for companies that own a large number of cable systems.

Network Telemetry
A technology that allows remote measurement and reporting of information. Although the term commonly refers to wireless data transfer mechanisms (e.g. radio), it also encompasses data transferred over other media, such as a telephone or computer network, optical link or other wired communications.

NOC – Network Operations Center
Pronounced “knock,” a NOC is one or more locations from which control is exercised over a computer, television broadcast or telecommunications network.

NTF – No Trouble Found
A term used in various fields, especially in electronics, referring to a system or component that has been identified for repair but operates properly when tested. This situation is also referred to as No Defect Found (NDF) and No Fault Found (NFF).

NPV – Net Present Value
In finance, the Net Present Value of a time series of cash flows, both incoming and outgoing, is defined as the sum of the Present Values (PVs) of the individual cash flows of the same entity.

Outage Risk
The likelihood that a service will be disrupted at some point during its transmission, preventing it from being delivered to its destination subscriber.

RCA – Risk Concentration Analysis
Material risks emerge when correlating risks from all silos and considering each in context. The RCA approach yields a Materiality Score, making it easy to recognize and prioritize material risks – the risks that matter. After collecting vulnerability data from throughout the business, RCA software assigns a score to each "risklet" that reflects its likelihood to cause a problem – as well as the impact that problem would cause.

Reputational Risk
Reputational risk is related to the trustworthiness of the business. Damage to a firm's reputation can result in lost revenue or destruction of shareholder value, even if the company is not at fault. Metrics used to calculate reputational risk in the Cable MSO world include the number of subscribers impacted, the number of services impacted and the number of outage minutes.

RGU – Revenue Generating Units
An individual service subscriber that generates recurring revenue for a company. Cable and telephone companies generally break down their subscribers into RGUs.

QoS – Quality of Service
Quality of Service comprises threshold requirements on all the aspects of a connection, such as service response time, loss, signal-to-noise ratio, cross-talk, echo, interrupts, frequency response, loudness levels, etc.

Truck Rolls
Refers to the act of dispatching a cable truck to resolve a service problem, usually at a home or street location. Truck roll volume is monitored closely by MSOs because it comprises a large percentage of operating expenditures.

UER – Uncorrectable Error Rate
A metric for determining the data corruption rate in a telecommunications transmission. UER is the number of data errors discovered after applying any specified error-correction method.

Sources: Rev2, Wikipedia.

About the Author

Robert F. Cruickshank III is the Chief Technology Officer at Rev2 (Valhalla, NY, http://rev2.com). Robert joined Rev2 from Cablevision Systems, where he was VP of the Customer Service Operations Center, spearheading deployment and use of next-generation solutions, including ARRIS ServAssure and Rev2 RiskView®.

At Cablevision, he had the pivotal role of simplifying Call Center tools with network health Go/No-Go metrics to streamline and efficiently deliver outstanding service to Cablevision's customers. Robert forged

communications among various teams including customer service, field operations, network operations and engineering. Prior to Cablevision, he spearheaded development of Network and Business Operation Support Systems at Stargus, C-COR and ARRIS, and led the development of the DOCSIS world standard cable modem at Cable Television Laboratories. Prior to joining the cable television industry he researched and prototyped ISDN Smart Building sensors at AT&T Bell Laboratories.

A veteran of the US Air Force, Robert was second in command of Lockheed C-130H Hercules cargo aircraft from 1987-1995. He received his undergraduate and masters' degrees in mechanical engineering from Worcester Polytechnic Institute. In addition, he completed five years of post-graduate work in Internet-based intelligent building energy conservation systems at the University of Colorado at Boulder.

Acknowledgement

The author would like to recognize the sharing spirit and pioneering Service Assurance work underway at leading MSOs.

###