Curbing Theft of Service Starts With Getting to Know Your Customer

Collecting customer data and comparing usage patterns can help utilities build models that accurately identify theft cases.

www.UtilitiesProject.com/10715

Theft of service has been discussed more in the boardroom in the last three years than it has in the past 30. Why all the new interest?

In short, the boardroom is responding to its perception of how some consumers may react to skyrocketing energy and resource prices. Unprecedented rates are pushing more consumers than ever before to resort to actions like stealing service. There is even word of an emerging market for professional "service tamperers," who are paid to assist consumers in bypassing metered service.

Skyrocketing prices aren't the only factor. Sarbanes-Oxley, competition created through deregulation, and the public and state regulator's demand for better corporate governance all contribute to making theft of service a 20th-floor topic.

No territory is immune and no service is safe from theft. With a little knowledge, a little nerve or the right contractor, anyone can tap into electric, gas and water services. The majority of theft occurs in the residential sector, but the majority of all revenues lost, estimated between 1 and 3 percent of total distribution revenues, occurs in the commercial account sector. A utility with $1 billion in revenues potentially loses between $10 million and $30 million each year to theft, and more than two-thirds of that loss is within the relatively small commercial account sector.

We will focus on commercial accounts to discuss how and where the most significant theft occurs and what leading North American utilities can do and are already doing to curb such illicit activity.

STEALING AROUND THE METER

The smarter thieves do not steal all of the service or tamper with the meter directly. This is an ill-conceived act with short-term payoff, since it's likely to generate a zero-read event at the utility.

Locking and sealing programs, solid-state meters and automated meter reading (AMR) tamper flags all help protect the meter but not the energy. A smart thief knows this and tampers around the meter instead.

AMR tamper flags do not detect bypasses that divert energy around the meter, while locks and seals do not prohibit theft outside of the meter box. Analysis of theft cases among Detectent's AMR-enabled customers between January and December 2006, revealed that most thefts occur without any corresponding tamper flag. Moreover, the majority of tamper flags triggered don't even indicate a theft case or any other spurious activity. Most of them are the result of normal daily activities, such as contractor-induced outages and maintenance service calls, as well as external factors like vibrations from nearby machinery. The enormous volume of false alarms tends to minimize the impact of those few valid tamper flags.

So the question is, how can a utility defend against theft of service when the thieves are getting smarter and the technology deployed does not address the major losses that occur outside of the meter box?

PROTECT THE SERVICE, NOT THE METER

Service protection is not achieved through locks and seals, although a locking and sealing program is an important component of meter security.

The service can only truly be protected by recognizing anomalous consumption. To do this, however, we first have to understand what consumers do with the energy and resources they receive. Then models can be developed to establish expected consumption patterns. Erroneous consumption patterns can then be detected as deviations from normal expected behavior. As a result, both theft around the meter and direct tampering can be exposed.

KNOWING THE CONSUMER

Customer information systems (CIS) were designed to facilitate customer identification and business transactions such as billing. They weren't designed to store the variety of data involved with getting

WRITTEN BY

Mike Madrazo, Detectent

Michael Madrazo is the founder and president of Detectent, the pioneer in developing analytical unmetered loss detection solutions. Prior to starting Detectent, he was the vice president and general manager of Invesys Avantis, an enterprise asset management software provider to power and process companies around the globe. Mr. Madrazo has a B.S. in mechanical engineering from California Polytechnic University.

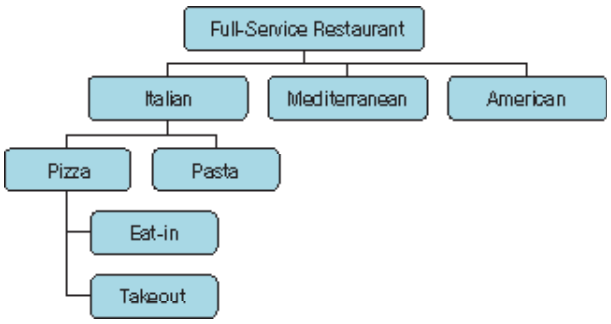

FIGURE 1 An advanced consumer model breaks down the standard industry code into more specific groups.

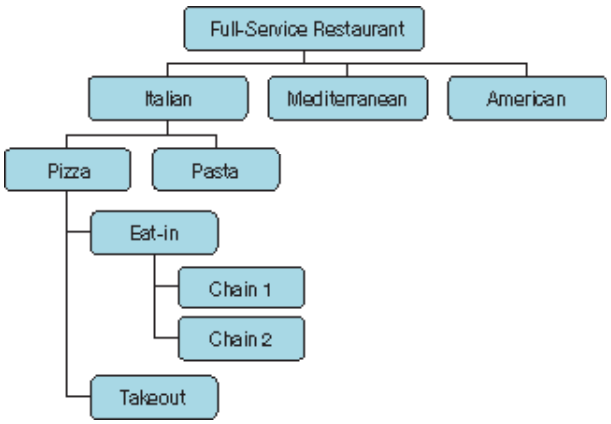

FIGURE 2 Chain affiliation lends additional detail to the consumer model.

to know the customer better. A great illustration of this is the classification of customers by standard industry code. A standard industry code of "full-service restaurant" provides no indication of how a restaurant uses energy and resources to fulfill the needs of its customers. With such simplistic coding, "full-service restaurant" can include everything from a large steak and seafood house to a small sandwich deli. Both use energy and resources in completely different ways to serve their customers.

If, however, the data indicated that the full-service restaurant was actually a pizza parlor with an eat-in area, an extrapolation on the energy needs of that restaurant could be made. For instance, you would expect to find a certain number of pizza ovens to meet the demands of a certain dining-area capacity. You would expect seating areas to be air-conditioned in the warm months and heated in the cooler months. You would also expect refrigeration in scale with the number of potential patrons served.

One approach to protecting service collects all of this information to create peer groups and predictive models.

CONSUMER MODELING AND PEER GROUPING

Basic consumer models take into consideration the standard industry code, but more advanced models expect that code to be broken down into greater detail. These models are designed to understand energy and resource consumption needs based on in-depth knowledge of expected usages. For the example shown in Figure 1, the broad category of full-service restaurant is refined by cuisine, then by a sub-type and, finally, into groups depending on the environment where the food product is served. When you break data down into subcategories, you can determine that the consumption of energy for, as an example, a takeout pizza restaurant is significantly different than that of an eat-in pizza restaurant.

The addition of chain affiliation can make these models even more precise in determining expected energy and resource usage, because most locations of the same chain will have standard equipment specifications. In Figure 2, expected consumption varies not only by the restaurant environment but also by the national chain that dictates the installed equipment specification.

APPLYING THE LOGIC TO OTHER BUSINESS TYPES

The restaurant example may seem like an obvious case for consumer modeling, but in reality, consumer modeling can be applied to all business types. Hotels and motels can be classified by number of rooms and leisure and business amenities provided. Gas stations can be classified by complimentary services such as car wash, shopping and restaurant facilities.

GATHERING THE DATA

The obvious next question then is, if the data does not reside in the customer information system, then from where does all this information about the consumer come? It might surprise you to learn that the information is gathered from a huge variety of publicly available sources.

The Internet offers access to vast repositories of information on commercial consumers. These are commercial entities that can create good will, and benefit in other ways from having the public know about them. All we have to do is know how and where to obtain that information for our own purposes.

WEBLINK

More information and additional material can be found online at www.UtilitiesProject.com/10715

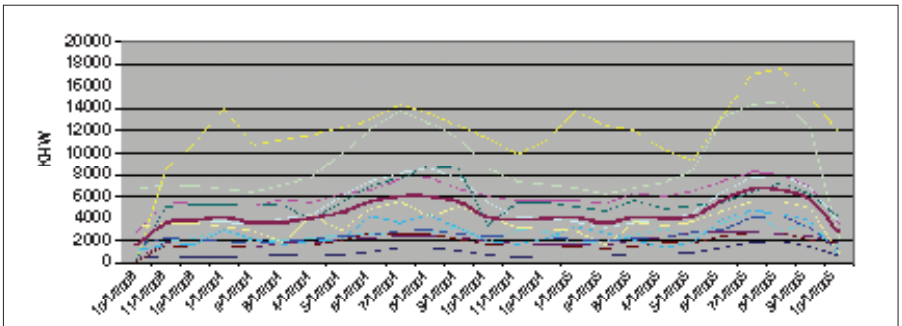

FIGURE 3 Actual Consumption Patterns Compared With the Expected Norm

There are numerous databases you can purchase that offer a wealth of information about commercial consumers, such as type of business, products and services offered; environment in which the products and services are offered; size of business; location; number of employees; hours of operation; sales volumes; and so forth. This information, once paired with data from the utility's own computer information system, provides quite a clear picture of how commercial consumers utilize the energy and resources delivered to them.

ESTABLISHING PEER GROUPS

Gathering data on a single consumer is only valuable if there is a like set of data on similar consumers available for purposes of comparison. Therefore, peer groups must be established and similar data elements must be gathered for each account in a peer group.

Peer groups can be developed for each service territory as well as nationally. Geographically, local peer groups may represent expected energy and resource usage more reliably, but national peer grouping offers a larger base with which to make comparisons, develop trends and establish expected norms. Figure 3 shows plots of consumption for various businesses of the same type against an expected norm calculated from the peer group's data. The expected norm is illustrated by the dark magenta line and outliers are considered those that do not follow the same pattern. Actual monthly consumption is not a significant factor, as this particlar grouping is not concerned with service capacity.

ELIMINATING FALSE ALARMS

It's possible to become overwhelmed with increases in false alarms as the volume of data being processed increases. This is especially true when comparing businesses based on expected similarities. Any number of things can change a business's consumption pattern such that it appears anomalous – changes in ownership or management, a shift in operating hours, an incorrect business classification, multiple meters under different names, seasonal conditions, closures for remodeling, even the simple act of upgrading equipment. The key to successfully identifying anomalous consumption is to filter out these false alarms through a process of screening and analysis.

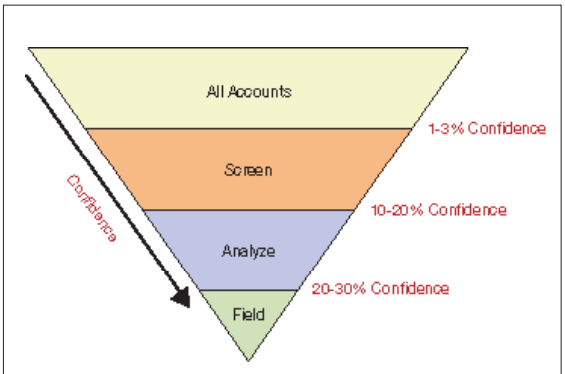

FIGURE 4 A screening and analysis process can pinpoint most false alarms.

Before a seemingly anomalous account is identified for investigation, it gets reviewed and verified for accuracy and any potential changes in how business is conducted. This process tends to catch most of the false alarms and eliminates false cases from investigation. Furthermore, it corrects the account's peer grouping to ensure integrity in other comparisons.

This process is illustrated in Figure 4. The confidence factor on the right side indicates the likelihood of a theft being discovered. The more thorough the screening and analysis, the higher the likelihood of success in the field.

OTHER SOURCES OF DATA

Another significant data source is to look at other services delivered. Whether delivered by one utility or by separate utilities, multiple service data can add tremendous value to the analysis process. A great example would be a Laundromat. A Laundromat typically has gas dryers and electric washers. If we know the usage of either gas, electric or water, then consumption projections can be made for the other services too. It is very safe to extrapolate this way because most Laundromat customers will use an amount of water and electricity in direct proportion to the amount of gas used for drying. If one of the services is not metered properly, it will show up as anomalous based on its ratio to the other metered services. Even if all services had been tampered with, the ratio of stolen service is not likely to be consistent, so it would still appear as anomalous usage.

These same energy use ratios can be developed and modeled for almost all business types, whether they're restaurants, hotels, service stations, public facilities, etc. Energy use ratios have consistently identified significant theft cases that date back years and would otherwise have remained undetected.

SUMMARY

Theft is not going away and is only likely to increase in the coming years. That's the bad news. The good news is that there are effective tools for identifying anomalous usage patterns. Data gathered in different service areas can be used to build consumer models and peer groups. By integrating data from AMR tamper flags with those models, valid theft cases can be identified more accurately. ■