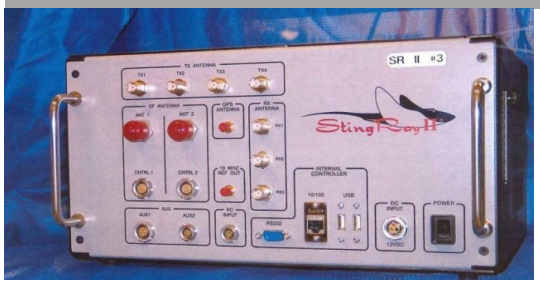
TMC's ADVISOR

Covering IT and Telecom from a Western Canadian Viewpoint — *March 2015*

The Sharing Issue: *the Good, the Bad and the Ugly*



An example of equipment that can be used to set up a rogue cell site. The entire set-up can fit in a van.

Just When You Thought You Were Safe—Fake Cell Sites

By Peter Aggus

People have reported that they've detected cellular base stations that don't belong to licenced cell carriers. These are rogue base stations and can be used to force a cell phone to connect to it and disconnect from their carrier. Without special equipment, the user has no idea that this has happened. So what are these fakes?

Read More

Inside

Shared Services as an Overlay- By Ellen Koskinen-Dodgson

IT departments everywhere share a common problem – an ever-increasing workload without a matching growth in staff. Transformational projects are routinely deferred in favour of 'keeping the lights on'. Here's an example of how to address this problem using a shared services model on an overlay basis.

A Marvel of Disaster Recovery -By Alan Bajkov

On April 19, 1995, the Federal Employees Credit Union (FECU) was destroyed as part of the Oklahoma City bombing. All IT infrastructure, all records and files and hundreds of thousands of dollars in checks and cash vanished. Of the 33 employees, 18 died, five were hospitalized, and many of rest were too traumatized to return to work...and yet, the FECU was open for business in just over 48 hours. Here's why.

Are You Too Trusting? - By Guy Robertson

Most business people are very good at what they do at work but they can be babes in the woods when it comes to IT security. When they lose their phones, tablets or laptops, it's often a result of their trusting nature. They're surprised when they're told that the loss was preventable.

Fake Cell Sites

By Peter Aggus

People have reported that they have detected cellular base stations that don't belong to licenced cell carriers. These are rogue base stations that can force a cell phone to connect to it and disconnect from the carrier. Without special equipment, the user has no idea that this has happened. So what are these fakes?

Cellular Basics

The cellular system relies on a network of base stations to link cell phones and other mobile devices. The cell carriers each has their own network, which operates on a dedicated set of frequencies that have been licenced to them.

An example of equipment that can be used to set up a rogue cell site. The entire set-up can fit in a van.

Each mobile device communicates with a cell site (usually a tower) using a pair of frequencies, one each for transmit and receive. A voice call or data connection is extended through the network and connects to the telephone network, the internet or another cell carrier. If the other end of the call is a mobile device, then it communicates to a local cell site using a different pair of frequencies.

A cell phone detects the strongest signal from a base station operated by its cell carrier and then automatically connects to it. A cell phone will detect other nearby base stations and as the cell phone moves around, it will drop its connection to its current base station and connect to one with a stronger signal in a process called 'handoff'. Each operator introduces new base stations into its network where demand has risen. This can even be done on a temporary basis for a large event with a 'cell on wheels' (COW).

Cellular calls are not easy to monitor. The system operates with digital encoding as well as frequent switching between channels.

Intelligent Monitoring

Law enforcement and other agencies now have access to their own fake cell sites; which can be operated from a permanent site, a van or even a flying aerial drone.

Operating as the 'man in the middle' allows them to hijack cellular traffic in an area and monitor it at will. They can recognize cellphones of interest and release other traffic back to the real network. By moving the cell site, they can pinpoint the location of their target.

The Real Problem

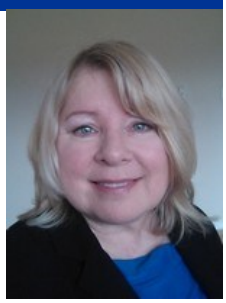
Whilst it may be OK for legitimate law enforcement agencies to use these tricks to catch the 'bad guys' - what happens when the bad guys get hold of the technology?

Consider what would happen if your competitor parked outside of your office with one of these devices. They could monitor or reroute your voice, data and text messages. Of course it's illegal—but when has that stopped industrial espionage?

This article is reproduced from the March 2015 edition of ***TMC's Advisor***

Peter, as an engineer and technology management consultant, has developed innovative and cost-effective solutions for clients in many industries.

Shared Services as an Overlay



By Ellen Koskinen-Dodgson

IT departments everywhere share a common problem – an ever-increasing workload without a matching growth in staff. Transformational projects are routinely deferred in favour of 'keeping the lights on'. Here's an example of how to address this problem using a shared services model on an overlay basis.

Shared Services—NIMBY

Organizations have traditionally had a 'not in my back yard' attitude towards IT shared services because it meant surrendering their IT department to an outside organization. The arguments in favour of shared services have real merit: "Why have dozens of separate groups replicating almost-identical services with 'never enough staff'?", but the downside is loss of control. Rather than having IT priorities match the organization's priorities, the entire organization now must compete for IT resources, making a case for higher priorities and not always succeeding. The BCcampus model uses an overlay approach that addresses a list of specific projects.

Randy Bruce, Chief Information Officer, Director, Student & Data Exchange Services

BCcampus

The byline for BCcampus is ***connect, collaborate, innovate***. For more than a decade, Randy Bruce has led the development of BCcampus applications and services as CIO and Director, Student & Data Exchange Services. His credentials are extensive: a B.Sc. - Computer Science (Honours) from UBC, M.Math – Computer Science from Waterloo, and a series of senior positions at Kwantlen University College including Director, IS and Computing; Acting VP, Education; and Dean, Information and Educational Technology.

BC Campus is tasked with making life easier, more economical and richer for students, instructors and program administrators. Their vision directs their services development and delivery, which include approximately 20 *Shared Services*, *Collaborative Programs*, *Student and Data Exchange Services* and *Curriculum Services and Applied Research*. Examples include:

- ***Adobe Connect***, which powers webinar, online meeting, mobile elearning, video conferencing and virtual classroom.
- ***Moodle***, a learning management system (LMS) used to complement face-to-face courses or deliver courses completely online.
- ***Open textbooks***, which significantly reduce student textbook costs while giving instructors the flexibility to customize their course material.
- A **federated identity** for students to simplify the application and transfer process throughout BC.

Is There a Lesson?

The BC post-secondary community has acquired a rich array of services using a shared IT service overlay approach. Could other sectors achieve a similar 'BC advantage'? Municipal? Resources? … It's a bold approach and well worth exploring.

This article is reproduced from the March 2015 edition of ***TMC's Advisor***

Ellen Koskinen-Dodgson is President and Managing Partner of TMC IT and Telecom Consulting Inc. She is an IT and Telecommunications Management Consultant, electrical engineer, author, speaker, media resource and Expert Witness.

A Marvel of Disaster Recovery

By Alan Bajkov

On April 19, 1995, the Federal Employees Credit Union (FECU) was destroyed as part of the Oklahoma City bombing. All IT infrastructure, all records and files and hundreds of thousands of dollars in checks and cash vanished. Of the 33 employees, 18 died, five were hospitalized, and many of rest were too traumatized to return to work…and yet, the FECU was open for business in just over 48 hours. Here's why.

Keys to Recovery

The restoration of the FECU was a marvel of disaster recovery. Three factors made this possible:

1. a sound and flexible disaster recovery strategy

2. the generous support of other credit unions and recovery experts

3. a spot of good luck as the three key people it most needed for recovery were available to work

FECU's disaster recovery strategy saved their systems and data. When the blast hit, a complete set of backups were shipped to a hot-site. The back-up provider brought in IT/telecom people and systems to the emergency site. Another Credit Union offered employees and the use of their new corporate headquarters. Volunteers from credit unions around the state pitched in and the FECU was back in business.

Lessons Learned

The story of FECU was a case of extreme disaster, both for the severity of loss in assets and information as well as for the unexpected toll in human life. Their experience provides us with insights and lessons about dealing with extreme disasters. Some of the lessons are:

- A good disaster recovery plan and off-site backups are mandatory.
- Where trauma plays a large role, the first priority of the executives has to be the physical and mental well-being of their people and customers. An outside source should handle as much of the logistical needs of the business as possible.
- Put out the word – ask for help.
- Media management is vital when customers look to the media for information about the well-being of that business.
- Maintaining communications for the executives, the consultants, and the trauma counselors was absolutely essential.
- The CEO for a business in the midst of a disaster such as this must **not be flooded by details** of the daily operations of the business**.** The Chief Executive Officers of the other Oklahoma City credit unions took turns acting as Florence Rogers' assistant during the crisis.
- Ongoing recovery testing – One example was that no one had realized that it would have been wise to take time for the backups to be copied before having them shipped to the hot-site. The information was irreplaceable, and luckily, none was lost or damaged.
- Use the opportunity to upgrade technology when replacing that technology becomes necessary.

This article is reproduced from the March 2015 edition of ***TMC's Advisor***

Alan Bajkov is a senior executive professional with over 30 years of experience with enterprise risk management practices covering IT governance and IT project management.

Are You Too Trusting?

By Guy Robertson

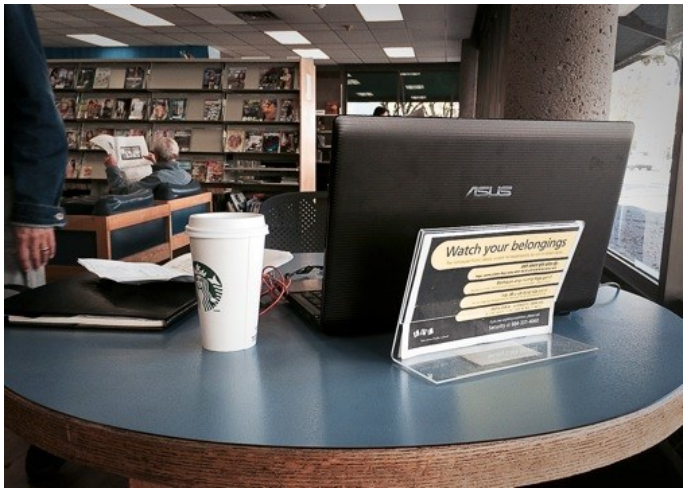
Most business people are very good at what they do at work but they can be babes in the woods when it comes to IT security. When they lose their phones, tablets or laptops, it's often a result of their trusting nature. They're surprised when they're told that the loss was preventable.

Let's say that I'm in competitive intelligence. That's a nice way of saying that I hang out in public places to pick up IT devices and sell the information. Sometimes I scoop items that travelers inadvertently leave behind. Sometimes I make phony claims at the airport's Lost and Found. Occasionally I steal items, such as the laptop left in a restaurant when the owner visited the washroom, or the BlackBerry left in a pocket on the coat-rack in the hotel's conference centre.

Don't Let It Happen

Be site-sensitive: Remember that thieves prefer those public places frequented by tourists and business travelers: airports, train and bus stations, hotels, restaurants and famous sites.

Never leave hardware of any size unattended: Before leaving your table to visit the washroom, put your cell phone in your pocket. Take your laptop with you into that tiny cubicle at the airport. Never underestimate the value of the data that you carry with you.



Be discreet: Don't flaunt your technology. Don't offer the person beside you on the plane a demonstration of your cell phone's capabilities. If you must use a laptop in a public place, make sure that no one can peer over your shoulder at the screen. If you discuss business over a cell phone, beware of eavesdroppers. Telling your VP that you're tired of lugging around a briefcase crammed full of negotiable paper is not acceptable on a cell phone at an airport.

Don't travel with technology that you don't need. It's one thing to pack an extra pair of socks. It's another to carry your entire client database. In fact, we tend to carry far too much data, most of which we'll never need. Take what you need on a business trip, but don't take your entire IT department.

If you're not using it, lock it away: Most reputable hotels have vaults or secure storage areas for valuable items including portable IT. Remember that thieves love hotels, and that despite increased security, theft from rooms and poolside lockers is still common.

Record serial numbers and add identifying marks: If your device shows up at lost and found, how do you prove that it's yours? In some parts of the world, the bureaucracy around a lost-and-found claim is so complicated that travelers will sometimes walk away without an item that definitely belongs to them. Filling out the forms might cause you to miss your flight.

Hide the logo– don't look like an attractive target: If you're carrying something valuable, don't pack it in Gucci. Avoid using your business card as a bag label. Why would you tell a thief that you're a senior manager?

This article is reproduced from the March 2015 edition of ***TMC's Advisor***

Guy Robertson is a Senior Management Consultant at TMC who specializes in emergency management and disaster planning. He has written extensively on emergency planning and IT security—hundreds of articles as well as a book with worldwide sales.