Case study • Education

Alcatel·Lucent

UNIVERSITY DETERS DATA THEFT

USING BREAKTHROUGH 'NONSTOP LAPTOP GUARDIAN' TECHNOLOGY

Revolutionary Alcatel-Lucent **OmniAccess 3500 Nonstop Laptop Guardian (NLG) provides round-the-clock management, security and remote control of mobile laptops, regardless of their power state and location.**

CHARLESTON SOUTHERN UNIVERSITY

To further support its campus-wide wireless Internet service and better protect student, faculty and staff data, Charleston Southern University is using new Alcatel-Lucent technology to allow the school's IT Department to remotely oversee, secure and manage wireless laptop computers, and 'lockdown' these devices if lost/stolen to prevent asset loss, and more importantly, protect critical data.

ADVANCED COMMUNICATIONS HEAVILY USED AT GROWING UNIVERSITY

Founded in 1964, Charleston Southern University (CSU) in the U.S. State of South Carolina is one of that area's largest accredited, private universities enrolling about 3,200 students. It's affiliated with the South Carolina Southern Baptist Convention and offers academic excellence in a Christian environment to all faiths.

It also offers technological leadership through free, campus-wide wireless fidelity (WiFi) Internet access. The university installed the system nearly seven years ago, one of the first schools regionally to do so. CSU further encourages new and current students to select WiFi laptop personal computers (PCs) to assist in their schoolwork as they fully utilize the benefits of wireless high-speed web access versus deskbound, hardwired PCs.

"Laptops are very attractive here because you can carry them anywhere and still have fast Internet service, whether you're in class, the dormitory or library," says Rusty Bruns, the school's Chief Information Officer (CIO). "They are also better suited to smaller spaces like residence halls."

CHALLENGES

- Wireless laptops heavily used
- Faculty/Staff devices hold sensitive data
- Data vulnerable to loss/theft
- Cannot 'lockdown' data if PC stolen/missing

SOLUTION

- Alcatel-Lucent **OmniAccess** 3500 Nonstop Laptop Guardian

BENEFITS

- Ensures laptops always available to IT staff
- Immediate 'lockdown' of compromised PC data
- GPS feature locates missing devices
- Deters laptop theft
- Saves/eliminates costs of replacing devices
- Allows secure, expanded use of WiFi web strategy

As a result, a progressive 'mobile atmosphere' prevails on campus. More than 70-percent of residential students and 100-percent of faculty now carry WiFi laptop PCs. All seven residence halls and every classroom, laboratory, administrative and support building on campus are served wirelessly.

THE 'BLIND SPOT' WAKEUP CALL

All this highly-advanced, laptop-based communication was not without one critical disadvantage. "Unfortunately, laptops are easily stolen," Bruns says.

Until last year, the university never had a laptop theft. But that changed early one morning when Bruns literally received a 1:00 AM 'wakeup call.'

"I was informed by campus security that one of our labs was broken into and laptop computers kept there were missing," he says. "It took me by surprise because this had never happened before. I had to hurry to the school and literally stand there helpless while local police investigated the situation."

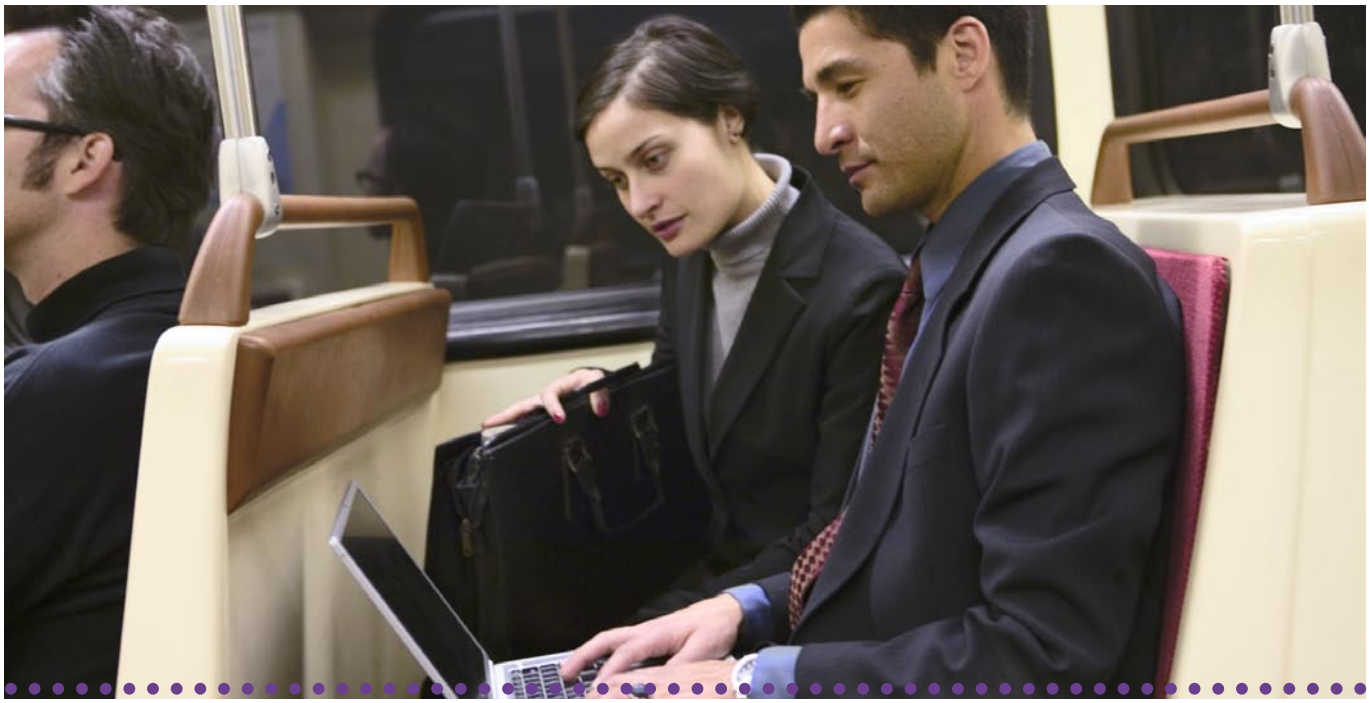
Fortunately, Bruns soon learned none of the missing laptops held sensitive personal or financial data: mostly student lab work and class notes. For a short while, it seemed the event would soon be forgotten with little impact on CSU's technological growth. However, the theft proved to have far-reaching implications. The first was monetary.

> The Nonstop Laptop Guardian lets IT professionals remotely oversee, secure and manage laptop computers to prevent loss of critical data.

PROFOUND COST AND CONFIDENCE RAMIFICATIONS

"Replacing the stolen laptops with in-kind devices was about $5,000 USD per unit," Bruns says. "Add to that some 'intangible' expenses such as staff time required to order replacement devices, re-install needed software, as well as students having to do without the laptops during shipping."

However, Bruns mentions there was another, more devastating consequence. "From that day forward, we no longer viewed our campus-wide mobile atmosphere with the same high level of confidence," he says. "We realized a WiFi-based laptop environment made us very vulnerable beyond hardware



replacement costs. Data on lost or stolen laptops is a major 'blind spot' because if the device is stolen, you lose all control over the information it contains."

At the same time, CSU's administrative staff was demanding expanded WiFi services for their laptops, and use of the devices was poised for even more growth.

"Despite the obvious risks, it appeared the campus community was willing to accept them in exchange for continued, open wireless access," Bruns says. "But as CIO, I was extremely uncomfortable with this tradeoff because losing sensitive administrative data would be catastrophic. We're no longer talking about lab projects and class notes: rather, detailed financial, academic, employment, security, payroll and personal information that could hurt the school monetarily and expose it to legal redress if not properly protected."

Since there was no quelling the demand for more laptops, CSU's IT group decided to aggressively investigate systems or technologies not only to stop laptop theft, but protect and control the sensitive data these devices store.

ALCATEL-LUCENT TECHNOLOGY A 'BREAKTHROUGH SOLUTION'

"As educators, we always emphasize that our IT professionals be knowledgeable of what's new and emergent in our profession, especially solutions that complement and enhance our IT leadership," Bruns says.

He was aware of new, prototype laptop security technology being developed by one of Alcatel-Lucent's research divisions, Alcatel-Lucent Ventures, located in New Jersey, USA. At a recent CIO Forum and Executive IT Summit in nearby Columbia, South Carolina, the conference coordinator knew of the school's situation and introduced Bruns to one of the key speakers, John Riggs, Director of Business Realization, Alcatel-Lucent Ventures. On further discussion, Bruns and his IT staff were receptive to field-testing the new product called the Alcatel-Lucent **OmniAccess** 3500 Nonstop Laptop Guardian (NLG).

> "NLG lets you take immediate control of a deplorable situation and turn it around to thwart those who caused it."
>
> **Rusty Bruns, CIO, Charleston Southern University**

The system consists of a unique 'computer on a card' that's installed in a laptop's PCMCIA card slot. Employing third generation (3G) wireless broadband technology expressly configured for data, each **OmniAccess** 3500 NLG has its own battery, memory, processor, operating system and software that links it to the laptop.

This ensures the protected laptop is always available wirelessly to the IT staff, working off its own battery power even if the laptop is switched off or the card removed from it. All laptops with PCMCIA slots are compatible with this new card.

"This solution answered our laptop security concerns, and fit perfectly with our major investment in WiFi communications."

Rusty Bruns, CIO, Charleston Southern University

The technology also increases the value of encryption solutions by protecting encryption keys on the card. If stolen or misplaced, the IT staff can wirelessly contact the specific card for the laptop, revoke the encryption key, and make all data stored on the encrypted drive unreadable.

If a missing laptop is later found, or located using NLG's Global Positioning System (GPS) feature, the encryption key can be enabled again, restoring all data and returning the laptop to full functionality. "This solution was the ultimate answer to our laptop security concerns," Bruns said, "and also fit perfectly with our major investment in campus-wide WiFi communications. With NLG, we can continue to encourage wireless laptop use and the high level of productivity these devices provide."

At present, CSU faculty and staff are provided NLG. A program to offer it to students at cost or at special pricing is being explored. Student grant funding for NLG is also a possibility in the future.

SECURING LAPTOPS SAVES MONEY/ELIMINATES WORRY

Being victimized is costly, says Bruns. "It is not just a matter of replacing stolen hardware and software, but the risks associated with sensitive data loss which can lead to more damaging activity, such as identity theft." He adds, "Now, as soon as I receive word of a lost or stolen laptop, I simply logon to the special Alcatel-Lucent web site, highlight the pre-registered entry for the device, and send the command to lock it down. The device is immediately rendered useless: the hard drive becomes inaccessible. Sensitive data can no longer be compromised. The only way to overcome this action is to turn it back on using the same NLG web site used to neutralize it."

Bruns calls the system's GPS feature 'incredible'. "The laptops stolen last year still haven't been found," he says. "But with the NLG's GPS tracking feature, we today stand a good chance of recovering a missing or stolen laptop and saving the costly replacement charges and wasted time to reorder and reload each device. That means everyone worries less about that dreaded, early morning phone call to report laptop theft."

Perhaps most important, Bruns says there's a powerful emotional advantage offered by this technology – the ability to quickly regain control, ultimately putting power back in the hands of IT.

TAKING POWER BACK A MAJOR BENEFIT.

"Let's face it. If you've ever had your car stolen or residence robbed, you know that depressing feeling of victimization," Bruns says. "Someone has violated your private property, and aside from alerting law enforcement, you are powerless to do anything more. That was precisely my situation the morning of the student lab break-in."

"Had NLG been available, I could have immediately entered the master web site and wirelessly locked down the stolen devices without leaving my home. If the thief tried to remove each laptop's card, the net effect would be the same – a valuable laptop PC with even more precious data inside would be rendered useless: an inoperable hulk of plastic and electronics. You can't put a price on the ability to be so proactive, as well as knowing that you've aggressively protected an asset," he adds. "You've taken immediate control of a deplorable situation and turned it around to thwart those who caused it."

Finally, Bruns credits this technology with solving one of his biggest IT challenges – how to further facilitate campus-wide WiFi mobility while closing the serious 'IT blind spot'. "Thanks to Alcatel-Lucent, we today have an unmatched ability to securely manage and control laptop devices 24/7, while protecting the data they contain," he concludes.

www.alcatel-lucent.com

Alcatel·Lucent