



Laptop Theft
in the
Commercial High-Rise

2005 Survey

BOMA Calgary Public Safety Committee

Calgary, Alberta, Canada

Table of Contents

Executive Summary	Page 3
Key Findings	Page 4
Facts We Learned	Page 18
Security Recommendations	Page 19
Other Considerations	Page 20
Conclusion	Page 20
Appendix 1: Tenant Lobby Checklist	Page 21
Checklist Explained	Page 22
Study Authors	Page 23

Disclaimer

The information provided at this report is intended to assist in educating commercial high-rise users with safe security practices and is designed as a basis for learning and for developing effective laptop theft prevention strategies.

It is not a guarantee that you will not be vulnerable to laptop theft. The BOMA Calgary Public Safety Committee is not responsible for thefts that arise as a result of anyone creating a program based on this report's findings.

Executive Summary

Laptop theft has always been a serious problem to property managers and tenants alike. However, starting in December 2004 there was a drastic increase from several laptops a year to several laptops a month being stolen. By June 2005, there were in excess of 100 reported incidents to police. And by years end, the Calgary Police Service estimated that in excess of 400 laptops and 50 LCD monitors were stolen from just the city's downtown core. Depending upon the equipment, information on the computer, lost productivity, lost opportunities, replacement costs, re-creation of lost work, insurance, and increased security measures, the losses were collectively measured in the hundreds of thousands if not millions of dollars.

As more and more thefts occurred, a concerned group of security professionals from the various property management companies came together to share whatever information they could. An extensive network of facility and corporate security, police and intelligence agencies across the province formed to share information, video footage and modus operandi of suspects. In addition, the BOMA Calgary Public Safety Committee members shared detailed information to create a roadmap of successes and failures of various thefts in order to determine what was stopping or not stopping this group of determined laptop thieves. This report is a summary of those findings.

Some of the general findings are the following:

- Multiple levels of physical and personnel security and procedures do work if properly applied.
- The average loss per event is in excess of several thousand dollars
- Rarely were stolen laptops recovered.
- Most victimized companies only spent money on security once several laptops were stolen.
- More important than the loss of equipment was the loss of morale and productivity of concerned employees of victimized companies.

Specific findings are detailed in the body of this report.

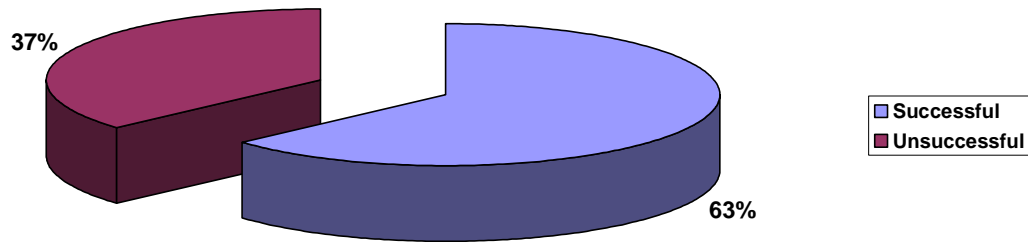
Appendix 1 displays a 'Tenant Lobby Checklist' which can be conducted by those interested in identifying weaknesses on individual tenant floors.

Key Findings

- There was roughly a 2 – 1 ratio for successful to unsuccessful thefts.
- There was close to a 50-50 chance of thieves gaining access once they have targeted a floor.
- In 73% of the incidents, access to the floor could be made via an unlocked stairwell door.
- In 62% of the incidents, break and enter was the method of entry.
- A variety of methods were used to gain access to the tenant space.
- Physical security was the primary method of stopping thieves.
- In 91% of the incidents, no CCTV was present on the floor.
- There was almost a 10 to 1 ratio of laptops to LCD projectors stolen.
- One third of all incidents occurred on a Friday.
- Almost 25% of all incidents occurred in August 2005.
- There were two main types of entry: defeating physical security and defeating procedural security.

There was roughly a 2 – 1 ratio for successful to unsuccessful thefts.

Overall Success Rate



There were 101 laptop theft related incidents documented throughout 2005.

63% of the incidents resulted in losses for the victim.

37% of the incidents were unsuccessful

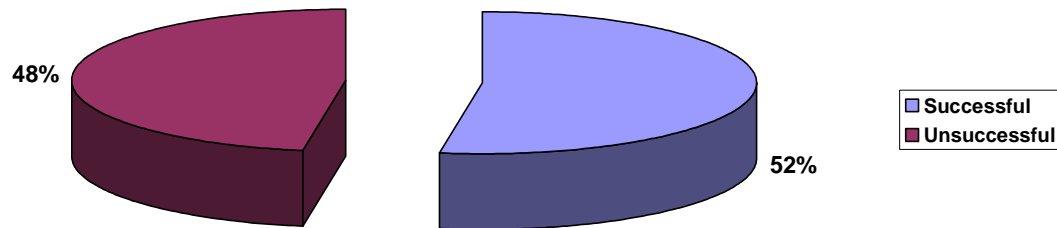
19 buildings across the downtown core of Calgary contributed information to this report.

9 buildings were targeted a total of 89 times while 10 buildings were targeted 12 times.

Number of companies targeted:	70
Companies targeted once:	53
Number of companies targeted more than once:	17
Total number of repeat victimizations:	49
Chance of being targeted once:	52%
Chance of being targeted more than once:	48%
Success rate of thieves for companies targeted more than once:	59%
Success rate for thieves who hit companies once:	66%
Success rate for thieves:	63%

There was close to a 50-50 chance of thieves gaining access once they have targeted a floor.

Break and Entry Success



Of the 101 incidents, 63 were break and enters or attempted break and enters.

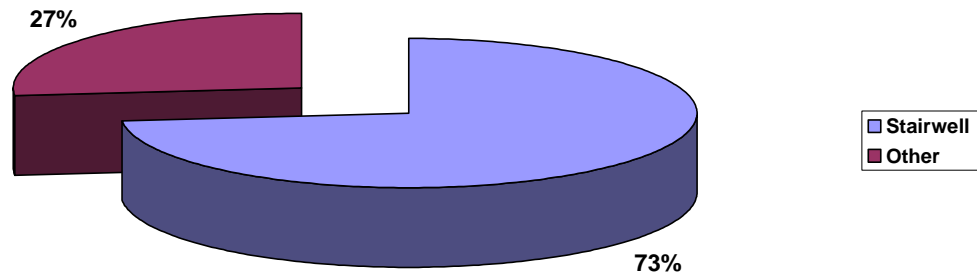
33 or 52% of the 63 incidents were successful
30 or 48% were unsuccessful.

In assessing the incidents, there was considerable evidence suggesting multiple layers of physical and procedural security, when effectively implemented, stopped thieves.

These multiple security measures included both physical and procedural including the use of CCTV on the tenant floor, astragals on doors, Electro-Magnetic Locks (EML's), deadbolts, alert employees challenging visitors, calling security personnel if concerned about visitors, staff not holding the door open for strangers and an over all security awareness program.

In 73% of the incidents, access to the floor could be made via an unlocked stairwell door.

Floor accessible via stairwell



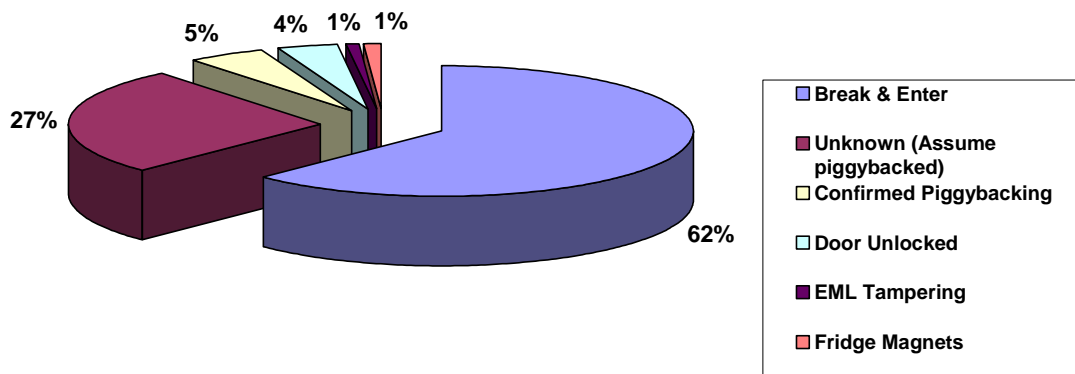
In 73% of the incidents, the floor was able to be accessed via an unlocked stairwell door. This does not necessarily mean laptop thieves used the stairwells in every case. However, there is considerable evidence to suggest they are using stairwells to travel between the floors, particularly after hours as elevator travel can be somewhat difficult for them. Stairwell travel is much more discreet.

In 27% of the incidents, the floor was not accessible via the stairwell door.

There is evidence thieves are entering buildings prior to lock up, accessed the towers via elevators to hide in washrooms and closets before coming out after hours to steal. They also accessed tenant spaces during regular business hours to steal. There was considerable anecdotal commentary regarding strangers being approached and questioned during regular business hours or staff having laptops stolen over lunch time. Some of the unknown individuals would leave the floor or leave the area. In some cases, building security personnel were called regarding these strangers and in other cases security personnel were not informed until the next day after several laptops were stolen.

In 62% of the incidents, break and enter was the preferred method of entry.

Method of Access



Whether successful or not, 62% of the incidents left break and enter evidence, the favored method of entry.

In 27% of the incidents, there was no evidence of break and enter. The assumption is that social engineering (the act of talking their way past opposition) or piggy backing (following in behind others without providing credentials) were methods of entry. However, thieves may have concealed their entry methods.

In 5% of the cases, it was confirmed that social engineering was the method of entry.

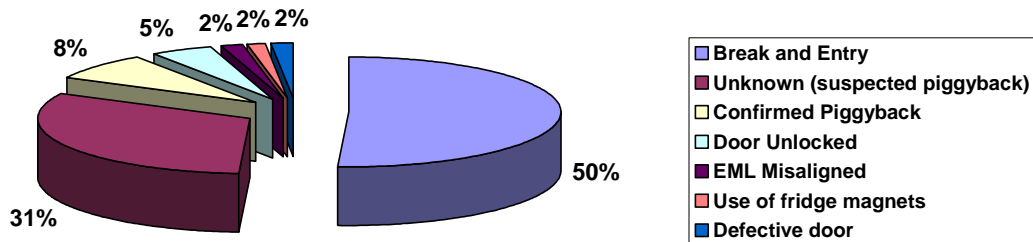
In 4% of the incidents, it was confirmed that a perimeter door was left unlocked.

There was one incident of definite evidence of Electro-Magnetic Lock tampering. What impact that had on the door is not completely known.

There was also one incident where a fridge magnet was found between the two halves of the EML. This would give the appearance of the door being locked while it was actually not.

A variety of methods were used to gain access to the tenant space.

Success Breakdown



At 50%, break and entry was the most successful method of gaining access to tenant space. There were several other methods including piggybacking, social engineering, doors found unlocked, fridge magnets placed between the 2 halves of electro-magnetic doors, and accessing defective doors.

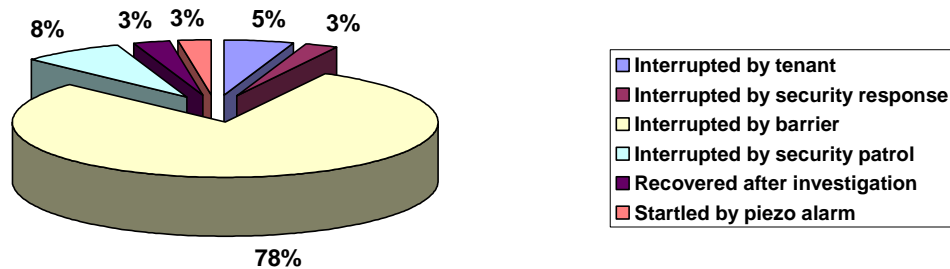
In 31% of the incidents, it is not known how entry was gained. However, there is strong indication that social engineering and/or piggybacking was used to gain access.

Strengthening procedural security should go a considerable way in reducing opportunists from accessing office space.

Procedural security includes challenging visitors, staff, contractors, and visitors wearing badges for identification, signing in visitors, escorting visitors at all times, and calling security personnel to assist in identifying unknown personnel.

Physical security was the primary method of stopping thieves.

Non-Success Breakdown



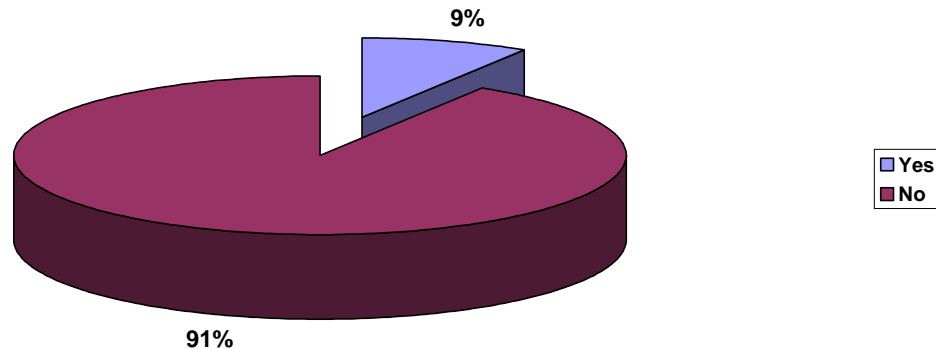
At 78%, the use of physical security barriers was the overwhelming method of stopping laptop thieves. This includes multiple layers of security including astragals or latch guards on doors, (preferably full length astragals), solid reinforced door frames, tenant lobby CCTV cameras giving good close ups (used for recognition purposes), mortise locks, laminated glass, Electro-magnetic locks placed on the tenant side of the door, properly installed and working access control systems including piezo (local door alarm buzzers), slab to slab covering with no crawl space above the drop ceiling, and rapid response by security personnel.

Security officer patrols were a distant second at 8%.

Other successful methods combined for a total of 14% included interruption of the theft act by the tenant, responding security personnel, conducting investigations and alarms. Interestingly, one laptop was 'found' two offices away from the original theft location two days after an investigation was launched, indicating in at least one case that the theft was precipitated by an employee. In one case, two suspected laptop thieves were challenged by an alert security officer in the main lobby and were escorted from the building.

In 91% of the incidents, no CCTV was present on the tenant floor.

Tenant CCTV Coverage



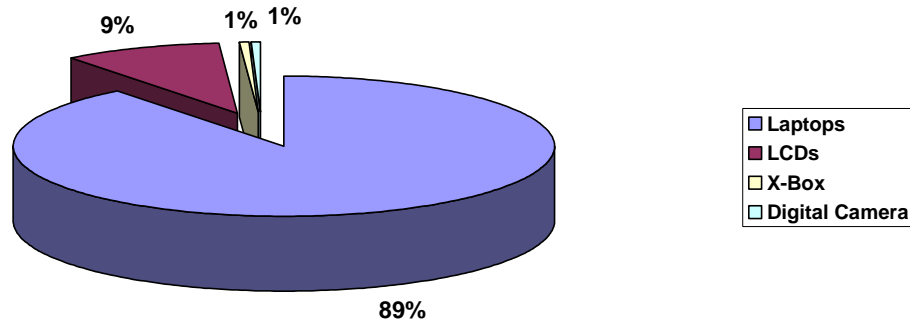
While it is difficult to prove a connection by a negative, there is strong evidence to support the contention thieves were bypassing tenant floors where CCTV was installed. While thieves do not seem deterred by CCTV in building common areas, they do seem to avoid the tenant floors with CCTV installed. One possible explanation of why thieves seem to not be deterred by common area CCTV include recognizing that connecting an individual on the ground or second floor to a theft several floors away, particularly in court may be impossible.

Several tenants reported observing suspicious activities by unidentified individuals, who, once they realized they are being observed, left the area and have not come back. Also, several tenants who had been repeatedly victimized, had all theft activities cease immediately once CCTV was installed. In several other cases where tenants were victimized despite CCTV, the local police were successful in identifying the perpetrator and arresting those individuals.

It should also be commented that there is a misconception regarding CCTV in commercial high-rise buildings. Building security were at times subject to unjust criticism by police and tenants regarding its lack of effectiveness. Due to the sheer size of many office towers, obtaining facial and body recognition is almost impossible. Cameras are used to capture gross movements of individuals and groups of people. Far more cameras would be required to capture evidentiary value video, on a scale outside the budget of most property managers and owners.

There was almost a 10 to 1 ratio of laptops to LCD projectors stolen.

Items Taken



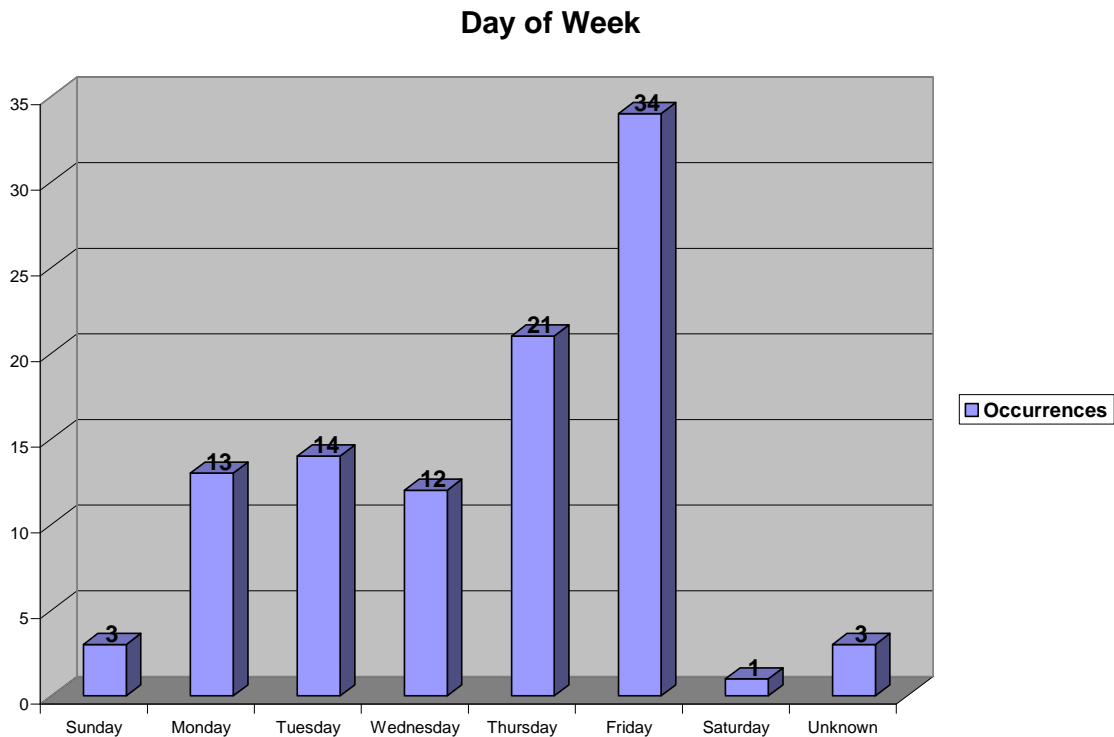
Of the total of 182 items stolen, there were:

- 163 laptops;
- 17 LCD projectors;
- 1 X-box,
- 1 digital camera.

The average theft resulted in the loss of almost 3 items gone for every incident. Each loss cost the victim several thousand dollars each. This does not take into account the lost information, the cost of replacing the computer and information and the cost of damage if it was a break and enter, etc.

There are mixed values associated with laptops and LCD projectors with the some claiming the street resale value of \$500.00 for a laptop while others indicating a laptop will be traded for \$40.00 worth of crack cocaine. LCD's are purportedly sold for \$1000.00.

One third of all incidents occurred on a Friday.



Of the 101 incidents:

34 occurred on Friday

21 occurred on Thursday

14 occurred on Tuesday

13 occurred on Monday

12 occurred on Wednesday

3 occurred on Sunday

3 occurred on unknown days and were reported that equipment went missing over the course of a week.

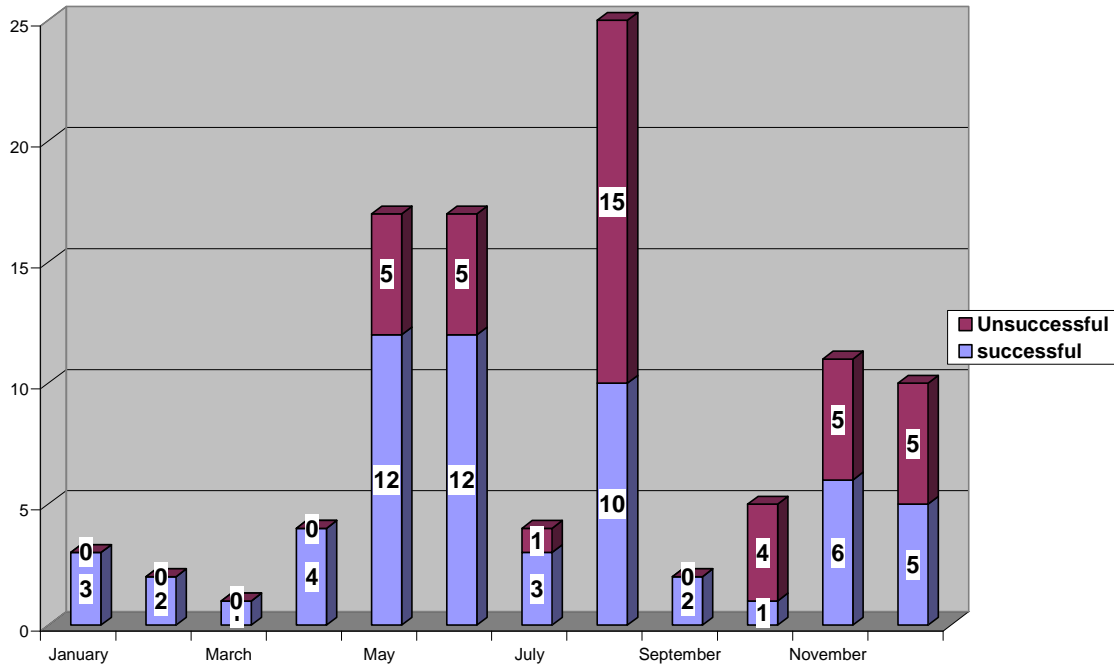
1 occurred on a Saturday.

One theory is that the 34% occurred on a Friday because these thieves are getting ready to party over the weekend and needed spending money.

Other possibilities include tenants may be in a hurry to leave on a Friday afternoon thereby more likely to ignore security protocols in their rush to leave. They have also been less likely to be working late, thereby allowing thieves more privacy and opportunity.

Almost 25% of all incidents occurred in August 2005.

Month of Occurrences



- 25% occurred in August
- 17% occurred in May
- 17% occurred in June
- 11% occurred in November
- 10% occurred in December
- 5% occurred in October
- 4% occurred in April
- 4% occurred in July
- 3% occurred in January
- 2% occurred in February
- 2% occurred in September
- 1% occurred in March

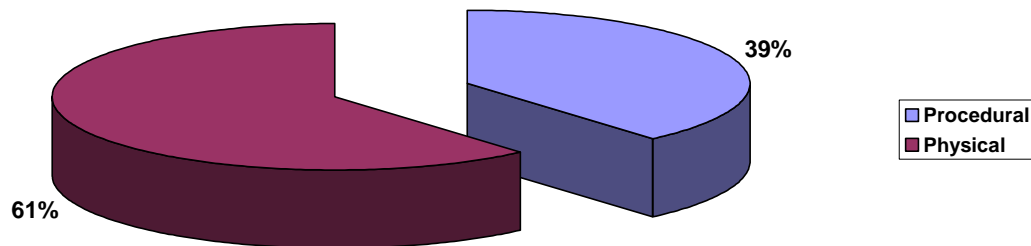
There is contention that as the popularity of laptop theft grew more and more thieves got involved, peaking with 25 incidents in August. It is interesting to note 15 of the 25 incidents in August were unsuccessful. There is a dramatic reduction in total number of incidents in September before another slow build up in the last quarter of the year. However, in the last 3 months of the year, with a total of 26 incidents, 14 were unsuccessful.

Successful to unsuccessful ratio

Jan: 3-0	Feb: 2-0	March: 1-0	April: 4-0
May: 12-5	June: 12-5	July: 3-1	Aug: 10-15
Sept: 2-0	Oct: 1-4	Nov: 6-5	Dec: 5-5

There were two main types of entry: defeating physical security and defeating procedural security.

Security Defeats



Physical Security Defeaters were responsible for 62% of entries.
Procedural Security Defeaters were responsible for 38% of entries.

There are 5 types of physical security defeaters:

1. B/E Artists attack the doors
2. Door Defeaters
3. Drywall Kickers
4. Door Jigglers:
5. Wall Jumpers

There are 2 types of procedural security defeaters:

1. Social Engineers
2. Piggy Backing

Physical Security Defeaters:

1. B/E Artists attack the doors

- Create their own opportunity: use blunt force.
- Tools include pry bars, bolt cutter and other tools;
- Have stolen both single and multiple laptops and LCD's;
- Break astragals, force doors from the frame, slip a slim-jim in the gaps between double doors or between the door and the frame;
- Can be defeated by high quality and multiple physical barriers including astragals, CCTV, solid wooden and steel doors, door alarms and laminate on glass insets.
- Door release motion sensors should be replaced with push-button releases.

2. Door Defeaters

- Will use a flat bladed pry bar and a mallet to force a gap between the two magnets on an Electro-Magnetic Locks.
- If given an opportunity, will place a penny, fridge magnet or other similar item between the halves of the door magnets to give the appearance of the door being closed.
- Inspection of the door required frequently.
- Conduct an audit of your priority alarms to reduce the number of false alarm so when a legitimate alarm comes in building staff can better respond.
- Doors need to be pulled on firmly to ensure they are closed.

3. Drywall Kickers

- Create their own opportunity: use blunt force to kick their way in through a wall.
- Walls can be reinforced by plywood, mesh or metal bars installed beneath the drywall.
- Have stolen both single and multiple laptops and LCD's;

4. Door Jigglers:

- Opportunistic
- Walk around accessing any doors found open or unlocked;
- Tenants need to be encouraged to close all doors firmly behind them, both entering and exiting premises.
- Need to be stopped and questioned.
- Anyone seen wandering around should be reported to building security.
- Security should rattle all door knobs on patrol to ensure the door is firmly closed.

5. Wall Jumpers

- Go up, through and over ceiling tiles into tenant space and other secure areas;
- You need to ensure slab to slab barriers are solid with mesh, additional dry wall, concrete, and other solid barriers.

Procedural Security Defeaters

1. Social Engineers: talk their way past employees
2. Piggy Backing: join the tail end of a group and enter surreptitiously.

Comments apply to both types:

- Look and act like they belong
- Possibly legitimate users including couriers, contractors, job seekers or those appearing to be.
- Depending upon the building, there are multiple entry points:
 - Building perimeter: doors
 - Elevator lobbies on the main and +15 floors
 - Elevators: both passenger and freight
 - Tenant lobbies
 - Parkade overhead doors and entry point for foot traffic
- Staff and contractors are encouraged to follow the rules ensuring others did as well.
- Ensure visitors are escorted at all times.
- Use a visitor sign in procedure.
- All employees should wear badges.

Facts we learned

- Minimum 18 - 20 thieves were operating in the downtown core, both male and female;
- Several worked in teams of two or more and communicated with each other via cell phone;
- When confronted, had good cover stories;
- Worked Mon-Fri using tenants and legitimate activity as cover. However, as of Nov 13, 2005 there were 3 confirmed Sunday thefts; thieves were again modifying behavior.
- Used building elevators prior to building lock up;
- Used the stairwells to move about once inside;
- Security precautions in cases easily defeated by an eager tenant or cleaner when they held the door open for others;
- Alarm management and a good working access control system were necessary;
- Contractors, tenants and other building residents, for whatever reasons, often refused to follow security procedures. Everyone must buy into the program;
- Good strong physical security measures can be effective in stopping them. Cases in point: of 38 attempts, 30 were defeated by multiple levels of strong physical security hardware.
- Focus was on the greatest Return On Investment therefore target hardening doors was important. As the tenant perimeter doors were the point of entry, security hardening had to begin there.
- Unlocked doors did not keep out thieves.
- Cable locks were ineffective, particularly after hours;
- Locking laptops in a cheap drawer while leaving the docking station sitting on the desk simply left broken cabinetry and missing laptops.
- The more valuable goods available, the higher the risk. Therefore one must evaluate the need for the best equipment;
- Initially only the highest-end laptops and LCD's were stolen. There were cases where B/E was completed but nothing taken. Later in August, low end laptops were stolen in a few instances.
- Thieves were waiting in stairwells just outside the tenant entry doors and when tenants exited, the thief quickly left the stairwell and entered the door.
- Some thieves conducted surveillance ahead of time, either hours or days earlier, so if there was a theft, security would check the CCTV at the time of the theft and back several hours to see if they could spot thieves who often covered their face at the time of the theft but sometimes not during pre-theft surveillance.
- The November 13 thefts suggested advance surveillance as 3 offices were attacked. All had exact same wooden door jamb. 2 thefts were on 1 floor in one tower and the 3rd was a different floor and tower.
- Large multi-tower complexes were far more likely to be broken into as all repeat victims have occupied space in this type of structure.
- +15 bridges, after reviewing the data were determined to be irrelevant to assisting in thefts.

Security Recommendations

- Tenant and Property Management together should conduct a thorough vulnerability analysis of tenant lobbies and should include:
 - Conduct slab to slab review: bring a ladder and flashlight;
 - Check all door locks, strikes, astragals, card readers and EML's and external mounted door pins for tightness;
 - Check for motion sensor shunts outside stairwell doors for proper settings.
- Program after hours elevators to wait up in the tower making requesters wait an additional 30-60 seconds;
- Consider the need for cross stairwell barriers;
- Consider CCTV for tenant elevator lobbies;
- 24/7 Card access to tenant floors except main reception;
- Procedures for visitors including badges for all staff and visitors;
- Reconsider who needs a high-end laptop;
- Investigate the feasibility of laptop vaults;
- Encourage staff to take laptops home.
- Multiple security layers are necessary. This includes Security Officers, CCTV, card select on elevators, cross-stairwell barriers, astragals, pin-pads, deadbolts, laminated windows.
- The need for a security information awareness program for employees and contractors is vital;
- Create laminated cards for cleaners explaining they cannot open doors and to contact security for entrance;
- Restrict access to floors to those on company business;
- Security staff should be aware that they may be watched in order to determine a routine. Patrol routes and times should be varied.
- Video surveillance and audible alarms should be at each access point to the building and individual business.
- Record all serial numbers and operating system service tag numbers. If recovered, there is a greater likelihood of property being returned.
- Information sharing amongst property owners and between security and police is crucial.
- Reinforce the door jamb with additional screws/fasteners
- For astragals, if you can get your finger between the astragal and the door or wall, it is too loose.
- Latch guards seem to be effective in stopping break and enters.
- Staff/security must be aware of doors being propped open and/or the placement of magnets on doors.
- Review the Laptop Theft Prevention Presentation developed jointly between CPS and private sector resources. <http://www.boma.ca>
- Security officers in tenant lobbies at key times can be a deterrent: primarily between 3 pm to 6 pm.
- Encourage staff to challenge visitors, conduct escorts, don't leave visitors alone to wander about.

Other Considerations

- Displacement (meaning they will try something different):
 - Time of commitment to attack;
 - Method which is used;
 - Object of attack;
 - Location of incident;
 - Type of offense.
- In early August/05 we started to see displacement of ‘object of attack’ and ‘method’. Older laptops and LCD’s were stolen and lever handles on doors were broke with a bar for attempted entry.
- Defense is not a one time tactic, we will counter their attack, they will change their attack and try something else.
- In November/05 we saw displacement of both day and methodology. Sunday thefts occurred and door jambs were attacked, neither of which had been seen before.

Hard Losses

Loss of Laptop
Replacement costs
Employee downtime
Loss of information

Soft Losses

Potential concern of staff
Loss of Reputation
Feelings of insecurity
Lack of confidence

A review of your organizations corporate I.T. back-up program processes is also required to ensure data is backed up regularly on servers.

A final consideration: All this costs money, some solutions are more expensive than others!!!!

Conclusion

Without multiple sound physical and procedural security measures in place, businesses will continue to suffer from laptop theft impacting the company financially on several levels. The loss of computer equipment has ramifications far beyond that of the immediacy of being unable to work. Companies need to recognize that security measures properly planned, instituted and enforced have a positive impact on business. Losses impact everyone and security is everyone’s responsibility. All affected groups including those both inside and outside the organization have a role to play in reducing laptop theft. Police, intelligence services, property management security, corporate security, I.T. personnel, facility people and individual employees all have a role to play.

Appendix 1: Tenant Lobby Checklist

PROPERTY	Day	Month	Year	Completed By:

FLOOR	Number of Doors	Tenants
		<input type="checkbox"/> Single (specify) <input type="checkbox"/> Multiple
Washrooms Public	<input type="checkbox"/> Yes <input type="checkbox"/> No	Slab to Slab Barrier <input type="checkbox"/> Yes <input type="checkbox"/> No
Stairwell Access	Elevator Access	CCTV Coverage
<input type="checkbox"/> Public Access 24/7 <input type="checkbox"/> Public Business Hours Only <input type="checkbox"/> Card or Key Access 24/7	<input type="checkbox"/> Public Access 24/7 <input type="checkbox"/> Public Business Hours Only <input type="checkbox"/> Card or Key Access 24/7	<input type="checkbox"/> Base Building <input type="checkbox"/> Tenant System <input type="checkbox"/> None

DOOR	# _____	OWNER/TENANT	Frame
			<input type="checkbox"/> Wood <input type="checkbox"/> Aluminum <input type="checkbox"/> Steel <input type="checkbox"/> None
Type		Construction	Window/Glass Insert
<input type="checkbox"/> Single <input type="checkbox"/> Double		<input type="checkbox"/> Glass <input type="checkbox"/> Wood <input type="checkbox"/> Metal	<input type="checkbox"/> Yes <input type="checkbox"/> No
Swing		Closes Secure?	Locking Mechanism
<input type="checkbox"/> In <input type="checkbox"/> Out <input type="checkbox"/> Both		<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Strike <input type="checkbox"/> EML <input type="checkbox"/> Lockset
REX Sensor	Exit Mechanism	Astragal	Lockset
<input type="checkbox"/> Open Door <input type="checkbox"/> Shunt Alarm <input type="checkbox"/> Not working <input type="checkbox"/> None	<input type="checkbox"/> REX Sensor <input type="checkbox"/> Exit Button <input type="checkbox"/> Door Handle <input type="checkbox"/> None	<input type="checkbox"/> 2-Bolt <input type="checkbox"/> 4-Bolt <input type="checkbox"/> Full Length <input type="checkbox"/> None	<input type="checkbox"/> Mortise <input type="checkbox"/> Classroom <input type="checkbox"/> Cylinder <input type="checkbox"/> Storeroom <input type="checkbox"/> Deadbolt <input type="checkbox"/> Dual <input type="checkbox"/> In Handle <input type="checkbox"/> Switch
Reader	Alarm Monitoring	Protectors	Damage
<input type="checkbox"/> Base Building <input type="checkbox"/> Independent <input type="checkbox"/> None	<input type="checkbox"/> Base Building <input type="checkbox"/> Independent <input type="checkbox"/> None	<input type="checkbox"/> Latch Guard <input type="checkbox"/> EML Box <input type="checkbox"/> None	<input type="checkbox"/> Door <input type="checkbox"/> Latch Guard <input type="checkbox"/> Frame <input type="checkbox"/> Reader <input type="checkbox"/> Handle <input type="checkbox"/> Strike <input type="checkbox"/> Pins <input type="checkbox"/> EML <input type="checkbox"/> Lock <input type="checkbox"/> REX Sensor <input type="checkbox"/> Closure <input type="checkbox"/> Exit Button <input type="checkbox"/> EML Box <input type="checkbox"/> None
Comments:			

Repeat checklist as necessary.

Checklist explained:

The tenant lobby checklist was designed to identify security vulnerabilities from a laptop theft perspective. It should only be completed by qualified personnel familiar with the various issues discussed. Any outstanding deficiencies should be identified and corrected.

Number of Doors: with more doors comes vulnerabilities as every door is a potential access point for thieves.

Number of Tenants: less tenants translates into greater unrestricted access to laptops and greater anonymity for thieves to move about without being challenged.

Washrooms Public or Private: publicly accessible washrooms allow thieves to hide easier.

Slab to Slab barriers: ensure tenant space is not accessible above the drop ceiling.

Stairwell access: thieves are using unlocked stairwells to move about unseen.

Elevator access: unsecured elevators allow unrestricted access for thieves in towers.

CCTV access on the tenant floor: indications are that thieves are avoiding floors generally which have CCTV. In some cases where CCTV was ignored it has been instrumental in arrests and convictions.

Door type: the more 'give' in a door, the more vulnerable it is, as thieves look for weaknesses to attack. Door frames can be spread apart and jamb's can be leveraged out. Metal doors and frames seem to be the most resistive to attack.

Closes secure: door needs to close and lock properly.

Locking mechanism: will be attacked. Where possible all components need to be heavy duty construction, resistive to manipulation from picking and blunt force.

REX sensor: improper installation leads to false alarms, failure to activate, or activation when not desired.

Astragal: full length preferred, 4 bolt next best thing. When effectively installed, denies access to the locking mechanism. Note, if a person can put their finger between the astragal and the door, then there is too much space. Astragals need to be close fitting and tight yet not interfere with the closing and latching hardware.

Lockset: should consist of hardened steel, resistant to attack with the right lockset installed for the required usage.

Reader: Should not be subject to manipulation and in proper working order.

Alarm Monitoring: real time monitoring with immediate response the best.

Protectors: helps protect hardware and door.

Damage: should be reported immediately with all damage, scratches, pry marks, etc inventoried and repaired as soon as possible.

Study Authors:

- Colin Best, Manager, Security Systems: Brookfield Properties.
- Sean Bolli, Manager, Security & Life Safety: Brookfield Properties.
- Les Cole, Manager, Security & Life Safety: Brookfield Properties.
- David Ellsworth, Manager Security & Life Safety: Brookfield Properties.
- Glen Kitteringham, M.Sc., CPP, Senior Manager Security & Life Safety: Brookfield Properties.
- Parnell Lea, Security Manager: CREIT Management.
- Ray McPhee, Manager Security & Life Safety: Brookfield Properties.
- Perry Smith, Manager, Security and Life Safety: The Cadillac Fairview Corporation Limited.

About the BOMA Calgary Public Safety Committee

The committee works within the commercial real estate sector providing security and life safety knowledge and expertise to help organizations protect their buildings and tenants. In addition, the Public Safety Committee works with outside agencies including police, fire and intelligence organizations as part of a network to develop standards, provide guidance and to increase public safety.