

The Laptop & PC Security Guidebook

Version #2



TRUE SECURITY INTEGRATION

A  FIRSTSERVICE COMPANY



Introduction

Due to their portability, relatively lightweight, and compact size, laptops are particularly vulnerable to theft. Safeware®, The Insurance Agency, Inc. estimates that 591,000 laptops were stolen in the U.S. in 2001. We estimate that approximately 60,000 laptops were stolen in Canada during the same year. Generally speaking, in our view, PC's are far easier to protect than laptops. This situation is exacerbated by the overwhelming desire of almost all employees to have a laptop instead of a PC. This is partially due to some employees seeing laptops as status symbols. Laptops, used by staff outside of the office, are even more at risk of being stolen because they are generally utilized in a less controlled environment than if they were used in the office.

Categories of Laptop and PC Theft

Organized groups and unaffiliated individuals are both actively involved in laptop and PC theft. They can basically be divided into four general categories. They are:

1. **Opportunistic Theft of Poorly-Protected or Unattended Laptops.** In the office environment, this often occurs at the start or end of the business day or over the lunch hour. Basically, anything that can be used to carry a laptop-sized object into an office can be used to carry a laptop out of an office. This includes briefcases, tool boxes, sport/gym bags, large purses, knapsacks, and even on some occasions, pizza boxes. The reluctance of most companies to search the bags of departing staff and visitors clearly favours laptop thieves. Such a policy has proven to be acceptable and effective only when it is applied to everyone including the CEO. Outside the office, laptops are most frequently stolen when they are left visible inside parked vehicles. As well, laptops are frequently stolen at hotels, airports and other transportation facilities. This is often done by way of a distraction such as two men arguing loudly and/or fighting near a ticket holder line up. A third member of the gang then commits the actual theft while the distracted ticket holders are watching the argument/fight. Pointing out money 'accidentally' dropped on the floor is also a popular distraction.
2. **Pre-Attack Probers.** Some criminals will probe (or 'case') the premises, during business hours, to locate a specific item(s) for which they have an 'order'. They will also evaluate any security aspects such as their proximity to an escape route(s), the alarm system (if any), closed-circuit television (CCTV) camera coverage, etc. At this time, probers will decide how many helpers are needed, where to park their 'getaway' vehicle, and most importantly, which point of entry is the best to attack. Pre-attack probes are often followed by an after hours burglary using multiple assailants and a stolen vehicle. Significant damage may be done to the premises, to ensure a short transaction time and rapid departure, **before** the police and/or security arrive in response to a burglar alarm. It should be noted that if, during the pre-attack probe stage, the criminal locates some (or all) of the targeted merchandise, and if the conditions are right (e.g., no witnesses and the 'loot' is close to an escape route), the pre-attack probe may just become an opportunistic theft.



Categories of Laptop and PC Theft cont'd

3. **Employee and Contractor Theft.** Minimal damage and a very clean crime scene are the hallmarks of internal theft. Generally, an access card and/or key will have been used to gain access to the premises. Some internal thieves may store the laptop on-site and come back after hours to remove it. For example, the laptop may be left above the ceiling tiles. Some internal thieves have been known to drop laptops and PC's out windows and into external shrubbery where they will be collected later. Sometimes the list of stolen items is consistent with an employee/contractor leaving to start his/her own business (e.g., one PC, one printer, one fax machine, etc.). The installation of CCTV cameras, at all exits, can help deter this group.
4. **Intelligence Gatherers.** These very skilled and well-trained thieves steal laptops and/or PC's that contain company information, which could be of interest to competitors, foreign governments, or other corporations/individuals interested in purchasing the subject company. This category represents the smallest number of thefts, 1% or less, but can potentially be the most damaging. Typically, the subject company will be high profile, a leader in its industry, and be working on projects considered revolutionary. The subject company may be involved in sensitive negotiations or extremely important tenders/bids. Perhaps the filing of patents may be imminent. They may do work for controversial or high profile clients.

Computer theft at a company such as this will likely have been preceded by more conventional intelligence gathering activities (e.g., in bars, on planes, or via 'ideal' job applicants). Pre-attack probes and surveillance may also have been conducted. These types of thieves are extremely careful and as crime scene analysis indicates, they have training and methods well beyond those of normal burglars. Sometimes the loss will not be readily apparent.

Targetted computers are often located a long way from escape routes and are usually found only in strategic departments such as Marketing, R & D, or Accounting/Finance. In some cases, the more expensive and/or more up-to-date computers have been left behind because the thieves were only after specific computers containing specific information. To reduce the potential for data theft, do not keep sensitive corporate data on individual workstations. This data should be restricted to server-based repositories, which can be secured in a highly controlled environment. Sensitive corporate, or personal, data should be encrypted. Please see our *Encryption Section*.

Many of the security solutions outlined in the following pages can be effective against intelligence gatherers. In addition, during sensitive times (e.g., during a takeover bid, before the launch of a new product, etc.) it may be prudent to upgrade security precautions. This may be done either by instituting pre-planned measures, as outlined in ***Intercon's 4-Level Security Escalation Planning Guide***, or simply by adding 24-hour Security Officer coverage until conditions returns to normal.



The Magic Bullet?

There is no single laptop or PC security solution. The successful laptop and PC security program will have many aspects including the following:

1. Access control.
2. Layering.
3. Target hardening.
4. Sensible policies concerning the assigning of laptops.
5. Education and awareness.
6. Meaningful key and access card control.
7. Ideally, **one** person (or group) in charge of laptop and PC **physical** security and another person (or group) in charge of laptop and PC **data** security.

When reviewing this document, or when receiving sales presentations, remember a wide range of solutions are required to produce the optimum solution for your premises. For this reason, our list of counter-measures is extensive and varied.

The First Step

Appoint **one** person, or a **small** committee, to be responsible for all aspects of laptop and PC physical security. This person, or committee, should report to a Senior Vice President or the Chief Executive Officer. All thefts of laptops, PC's, and associated equipment should be reported to them. In our experience, physical security is low on most IT departments' priority list. Also, where/when laptop and PC security is deemed to be 'everyone's responsibility'; it really is 'no one's responsibility'.

Who Does NOT Need a Laptop?

Unfortunately, almost all employees feel that the laptop is more desirable than a PC of equal (or greater) capacity. A large part of the laptop loss prevention program is to tactically decide who gets a laptop or a PC. From a **purely** loss prevention perspective, the following employees should **NOT** be issued laptops:

1. Employees who do not work outside the office.
2. Employees who work at a cubicle, carrel, or any work area that does not have a lockable door.
3. Employees whose work area is close to escape routes or exits.
4. Employees who work in public or semi-public areas such as reception desks or service counters.



Who Does NOT Need a Laptop? cont'd

5. Employees whose work area is constructed whereby the laptop would be located within 40 inches (one metre) of burglar-accessible, unprotected, grade level, exterior or interior (i.e., corridor) glass.
6. Employees whose work area lacks any form of access control and members of the public can wander in at will. This includes work areas where there is no receptionist and where card readers or biometric readers, etc. are not used to prevent unauthorized persons from entering.
7. Employees in sensitive departments such as R & D, Accounting, etc.
8. Employees who have previously had their laptops stolen from the office.

Naturally, most employees will be disappointed if their laptop request is turned down. Some non-travelling employees may state that they are requesting the laptop to work at home. In these circumstances, if the employee's workload warrants it, consider buying him or her a second PC for home use. In most cases, this is less expensive than purchasing the employee a laptop. It is definitely less expensive than buying them a replacement for a stolen laptop. Employees should sign an agreement that requires them to return the laptop/PC when their employment ends.

Records

It is important that up-to-date records of laptop and PC assignments be maintained. These records should include serial numbers, model numbers, numbers of all peripheral devices, cost, etc. In addition to hard and soft copies on-site, up-to-date hard and soft copies should also be kept off-site. The police (and insurance companies) require these numbers in the event a laptop or PC is stolen. As well, the police can use these numbers when trying to return 'recovered' property to the rightful company.

Identification

Laptops and PC's should be physically identified as company property. **Before** doing this, review the warranty for each specific piece of equipment. This is in order to determine if the modifications you are considering void your warranty. Identification methods vary from very subtle (e.g., engraving or branding the company name, or inventory control number, onto the frame, to painting the laptop or PC a very bright colour such as fluorescent orange or chartreuse). A Northern Ontario school board used the latter tactic and they believe it has dramatically reduced computer theft from their schools. Available marking systems include etching, engraving, foil labels, laser marking and ink that is visible only under ultra-violet light. (**Note:** *Some suppliers are listed in our Security Devices Section*). Police services also offer confidential property numbering systems such as 'Operation Provident'. Contact your local police service for details.



Identification cont'd

All users of laptops should insert a business card into the business card holder found on most new laptops. This will help ensure that you get your laptop back if, for example, you are attending a conference and many of the delegates are using the same laptop as you. Inserting a business card into the battery compartment is also recommended. This **may** assist the police in returning your laptop to you. Personally-owned laptops should also be engraved with a property identification number, possibly the Social Insurance Number (SIN) of the owner. Since this may increase the potential for identity theft, or otherwise make the owner's information more accessible, users of personal laptops should consider utilizing 'Operation Provident' or other commercially-available numbering system. Persons using their own laptops, for work outside their 'home office', should review their coverage with their insurance provider. This is in order to determine if theft of their laptop, while working in the field, is covered under their policy.

Laptop Movement Audits

Replacing employees' laptops with PC's **before** thefts occur is very difficult. To help justify this decision, conduct routine laptop movement audits. This is done, after hours, by applying a seal, label, or piece of tape to the back or underside of the laptop. Same should also be applied to the table, counter, or workstation the laptop is sitting on. Ideally, the tape (or seal or label) should **not** be readily visible. The tape (or seal or label) should have the date, time, and initials of the person who applied same. The tape (or seal or label) should be checked at pre-determined intervals (e.g., daily, weekly, or other appropriate time) to determine if it is still intact. If it remains intact for an extended period of time, the employee is likely **not** removing the laptop from the office. A PC may be more appropriate for this employee, especially if their work area lacks access control or is otherwise vulnerable.

Laptop Monitor

Where/when employees have been advised to follow certain security protocols (e.g., locking laptops in furniture or using cable locks) when leaving their work area, a monitor (or monitors) should be appointed to conduct regular inspections. If, during these inspections, the monitor(s) find exposed and unattended laptops they should leave written notification and remove the laptops to a pre-determined, secure lock up. The employee, regardless of position or title, has to make an appointment to attend the lock up to personally recover their assigned laptop. Ideally, the person responsible for the 'pick ups' will **not** be conducting the 'returns'. Persons assigned this duty should report to the CEO (or other very senior person) in order to protect them from reprisals. In some large corporations, multiple violations of this policy can result in disciplinary action.



Furniture

If laptops are not otherwise secured, it is prudent to advise employees to lock them in furniture when not in use. This removes the laptop from view and adds a layer of physical protection. While this is sensible advice, if a pre-attack prober has visited the premises they may assume that the laptop is locked away in the employee's furniture at the location where/when they first saw it. Also, most workstation furniture is not sturdy enough to resist forced entry by a determined, and often 'energized', assailant. Furniture utilized for this purpose should be tested/evaluated, for resistance to forced entry, **prior** to being used as a secure storage location. Local police crime prevention personnel may be able to assist with these tests/evaluations. A secure laptop storage compartment, with reinforced walls or drawer fronts and stronger locks with reinforced strikes, may be required at some workstations. Generally speaking, short and sturdy cam lock strikers are harder to bend than long, thin ones. Materials suitable for reinforcing furniture include $\frac{3}{4}$ -inch plywood and 1mm (or thicker) metal.

Work Spaces With Doors

Employees' assigned laptops, and who have work spaces with doors that lock, should be advised to lock their doors whenever they are leaving their work area. To facilitate this recommendation, consider the installation of free access, storeroom-function, lever-style, locksets. These locksets permit free egress (exit) but always lock upon closing. Locking hardware for offices containing laptops or PC's should be commercial grade 2 or 1 (preferable). Commercial grade 3 locksets are **not** as resistant to forced entry and are **not** recommended.

Layering

Laptops and PC's are best protected by the sensible use of the 'layering' philosophy. Ideally, a potential thief will encounter two, three, or more layers of physical protection and/or access control **before** they can get their hands on your computer. Multiple layers of protection and access control will increase transaction time and will increase the criminal's fear of discovery or capture. For example, if a thief only has to go through one entrance door, which may be unlocked during business hours, to get to your computers, then they are vulnerable. If the thief encounters a locked, or reader-controlled, door to the main office interior from reception, a locked door to the office containing the PC, and a plate lock on the PC itself, there is a greatly reduced potential for the thief to be successful.



General Guidelines

1. Laptop and PC hard drives should **not** be deployed within 40 inches (one metre) of any grade level, perimeter glass. Where this is unavoidable, the glass should be equipped with ACE/Security Laminates™ (or the equivalent) security film. This film, when applied to windows with suitable framing, will delay an assailant for up to 20 minutes or longer. When used in conjunction with suitable alarm system glass-break sensors, an attack can be detected and responded to **before** entry is obtained. The visual effect is minimal with security film and it does **not** convey a 'siege' mentality like bars. Since many break-ins, possibly up to 60%, involve entry through glass, security film should be considered for **all** grade level, exterior and interior, glass where a burglar could break same to access your computers. Rolldown, metal shutters, scissor shutters, or bars (constructed from 3/8-inch, or thicker, steel are acceptable). The general rule of thumb for bars is that the burglar should have to cut **at least two** or more in order to gain entry. Exterior-mount bars should be installed with one-way, lag screws or carriage bolts. Interior-mount bars are preferable. Where interior aesthetics are not a concern, it is useful to have drapes or blinds cover the bars so that they are not visible from the exterior. Breaking the glass and setting off the glass-break alarms, without obtaining entry, will surprise the burglar and will increase his/her transaction time, which may deflect them to another target.
2. Exterior (or vulnerable interior) doors, to areas containing laptops and PC's, should be solid core (versus hollow), planked wood at least 45mm (1 3/4-inches) thick or folded sheet metal, also 45mm thick, which utilizes sheet metal at least 1mm thick (or 1.3mm thick if constructed from aluminum). Most fire-rated doors meet these specifications. Stiffened doors are recommended, especially if magnetic locks are to be installed or where/when the premises has been previously attacked. Where the door opens outward, non-removable hinge pins or hinge cross pins are recommended. Strike cover plates are recommended for any outward-opening door where the lock strike could be pried back into the door.
3. If your computers are visible through grade level, perimeter glass, consider replacing landscaping river rocks (if applicable) with bark chips or mulch.
4. Plant 'hostile' vegetation such as shrubs with thorns (e.g., Russian Olive or Firethorn, etc.) under vulnerable windows. Please see ***Intercon's Tactical Landscaping Guide*** for more information on this topic.
5. As indicated in our *Who Does NOT Need a Laptop? Section*, employees working in public or semi-private areas (e.g., reception, mailrooms, service counters, etc.) should **not** be issued laptops. In our view, the most secure equipment for these areas are PC's that are secured with an enclosure lock (preferable) or plate locks. Ideally, the enclosure lock should be visible. This **may** act as a deterrent to pre-attack probers who, after seeing same, may assume (rightfully or wrongfully) that all PC's are secured in the same manner. Also, consider 'head' (aka 'chip') or 'drive' locks for these PC's. Please see our *Security Devices Section* for more information on enclosure locks and plate locks.



General Guidelines cont'd

6. During (and after) business hours, laptops that are going to be left unattended, in unlocked general office areas, should be placed inside lockable furniture. If they are going to be left on a desk, workstation, etc. they should be secured in place. Options are listed in our *Security Devices Section*.
7. Issue access cards and keys on the basis of 'least access necessary to perform a specific job function'. If possible/practical, avoid issuing master keys and access cards that provide access to **all** areas. Superfluous access is a definite security liability when keys and/or access cards go missing. (**Note:** *Please also see our Access Control Guidelines Section*).
8. Ensure that all contractor, visitor, and cleaner keys and access cards are signed in and out on a daily basis. A daily audit/reconciliation of **both** keys and access cards is recommended. Consider an exchange program (i.e., trade the key or card for a driver's license). If contractor or cleaner keys have left the site for an extended period of time, consider re-keying the area(s) in question. This is important if low security keys (e.g., Schlage™ or Corbin™) are in use. The use of restricted keys, as described in *Item #9*, reduces the need for this time-consuming, and potentially costly, measure. As soon as a card lent to a visitor or contractor is discovered to be missing, void it. Cards issued to contractors and visitors should **not** have 24-hour access.
9. Establish and enforce sensible key controls to help prevent employee and contractor theft. All areas containing laptops and PC's should have restricted keys. This means that only a licensed locksmith, upon receiving an authorized letter from the client, and utilizing special equipment, can cut these keys. The purpose of this measure is to prevent the unauthorized duplication of keys. The locksmith should stamp **all** keys with a unique, identifying number when same are cut. Employees should then sign for each numbered key they receive. **At least annually**, all employees should be asked to physically produce the key(s) they originally signed for. This is called an as-issued key inventory. If keys to areas containing laptops or PC's are lost or stolen, these areas should be re-keyed promptly. (**Note:** *Medeco™, carried by Intercon, Primus™, and ASSA™ are just some examples of these types of restricted, high security keys*).



General Guidelines cont'd

10. In many cases during the business day, it may not be feasible and/or practical to control all access to all areas containing laptops and PC's. Offices with no reception area coverage are vulnerable in this regard. Where/when this is the case, consider implementing some, or all of the following:
- a. Remove or lower any partitions located close to access/egress points. This will improve visual supervision of the access/egress point.
 - b. Assign some naturally suspicious, assertive employees the responsibility of challenging strangers and generally enforcing access control. Ensure that these duties are included in their job description and that their workload allows them to do this. Also, it is very important that their desks be oriented towards their 'assigned' access/egress control point.
 - c. To help ensure their safety, these employees should be trained in non-violent conflict resolution, stages of anger, and the use of code words in order to discreetly summon assistance in the event of an emergency. Consider the installation of duress buttons for employees assigned to this task.

CCTV

Interior and exterior entrances/exits (escape routes), to/from areas with a significant number of laptops and/or PC's, should be monitored via recorded, CCTV cameras. **Before** the purchase and installation of any CCTV cameras, define their exact purpose and intended result. Consider both overt and/or covert cameras for these locations. Overt cameras should be enclosed in vandal-proof, smoked domes, which are mounted high enough (10+ feet/3+ metres) to make tampering difficult. Since clear, high quality video records can secure offender convictions, it **must** be understood that obtaining more detail in an image is achieved at the cost of each camera covering a smaller and well-defined area. Recording equipment should be located in a less than obvious and secure area where it will be difficult for a burglar to find. In premises where this may not be possible, leave a 'live', decoy VCR in a closet where a burglar would most likely look for same. Ideally, they will take or destroy the decoy VCR and leave your genuine video records intact. To reduce the potential for incomplete video records, and to eliminate changing tapes on an on-going basis, utilize a digital video recorder (DVR). Whether a digital or analog recording medium is selected, it **must** be carefully specified to ensure the required image resolution necessary for success in court.



Plausible Cover Stories

Staff phone directories, located at office access points, should **not** include positions, titles, or departments. Also, where/when corporate culture requires names on offices; department and position/titles should **not** be included. For example, this information can be very useful to a computer thief when he/she is challenged if 'caught in the act' of carrying out four or five laptops (e.g., "Sir, where are you going with those laptops?" "I'm installing a software fix for Barb Smith, VP of IT."). By the time the well-meaning employee calls Barb for verification, the thief will likely be long gone with the laptops. Having a plausible cover story improves the thief's confidence level, which may embolden them. As well, when this type of information is readily available, the thief is much less likely to attract attention by, for example, not having to ask the receptionist who the head of IT is. Receptionists should be instructed to advise security, or their manager, when this type of inquiry occurs.

Visitor Badges for Laptops

In secure environments, it may be appropriate to issue visitor badges to visitors **and to their** laptops. Security Officers, at access control points, should record details such as the make, model, and/or serial number, etc. of all incoming laptops. When visitors depart, Security Officers located at egress points should ensure that they are departing only with the laptops they brought in with them.

Packaging Disposal

After receiving new computer equipment, dispose of the empty boxes (and other packaging) in as discreet a manner as possible. Consider removing address labels. If boxes cannot be disposed of by compacting, turn them inside out and tie them together. Some 'steal-to-order' (pre-attack probers) thieves drive around industrial sub-divisions looking for empty boxes that contained items they wish to steal. This same advice applies to people living in residential areas. If you have purchased and received a big screen TV, new PC/laptop, stereo system etc., break up the box(s) and/or reverse same **before** you put it out with the garbage or in the recycling bin.

Access Control Guidelines

In areas with a large concentration of PC's or laptops, doors at all access points should be controlled. Options include locks and keys, cypher locks, biometrics (with smart card authentication tokens), or card readers. In our view, card readers, interfaced to suitable electronic locking devices, is the preferred option. Card access control technology allows for the quick voiding of missing, lost, or stolen cards. Unlike cypher locks, there is always an audit trail of card usage. Another cypher lock problem is that to void the code, a new code has to be distributed to **all** users. This can be very time-consuming. Also, codes can be exchanged between users without any record of same. The main drawback with locks and keys is the inability to limit access by time zone (also a problem with cypher locks) and the lack of an audit trail of key usage. Where a record of egress is required, install out (exit) card readers. If no record of employee egress is required, install exit buttons. Exit buttons should be installed **at least 40 inches (one metre) away from any glass**. This is to prevent a burglar from breaking the glass and reaching through to activate the exit button, which would then open the door.



Access Control Guidelines cont'd

Maximize the use of the access control system. Only turn the system off protection when the premise is staffed and/or when the receptionist is on-duty. In many office towers, the building's access control system goes off protection at 7:00 a.m., which means that the elevators no longer require an access card to move between floors. As well, some or all of the stairwells may also unlock at 7:00 a.m., which leaves another access/egress route unprotected. If your company is a tenant in one of these buildings, and your office and receptionist hours don't start until 8:30 a.m., it makes sense to keep the elevators on access control until 8:30 a.m. and unlock the stairwells at the same time. This reduces the potential for 'tailgating' and 'piggybacking'. It also helps ensure that if a stranger does access the office, there will be lots of employees on-site to intercept, challenge, or deter them from criminal activity. In some theft-prone offices, where/when there is no receptionist relief, the elevators are put back on access control over the lunch period (i.e., 12:00 Noon to 1:00 p.m.). Additional ways to maximize the access control system follow:

1. The building and access control program should be designed with the objective of ensuring that as few as possible, unsupervised, non-employees have access to areas containing numerous laptops and PC's. Ideally, there should be **no** opportunities for unsupervised access into these areas.
2. Card readers, biometric readers, or personnel should control all entrances to areas with large numbers of laptops and PC's.
3. All visitors should have to sign in and out and wear a date-stamped badge.
4. Only certain, designated employees should be permitted to authorize visitors.
5. Employees should be instructed to challenge and/or report all unknown persons **not** wearing a visitor's badge in, and around areas containing laptops and PC's.
6. Consider an escort program for new or unknown visitors, especially contractors.
7. Eliminate the need for couriers, and other delivery personnel, to wander throughout open office areas. This can be accomplished by locating mailrooms close to an exterior entrance, installing card readers, or otherwise controlling any internal doors near mailrooms, which provide access to internal areas.
8. Employees and company personnel enforcing access control should be alert for disguises (e.g., a courier company baseball hat, a clipboard, cursory explanations, etc.). Ask these people open-ended questions: "Who are you here to see?" is much better than: "Are you Mary Smith's 4:00 p.m. appointment?" Be persistent. Do **not** be easily 'blown off'. Laptop and PC thieves will often try to resemble movers, couriers, repairpersons, plant maintenance staff, etc. Ask for an official company photo ID.



Access Control Guidelines cont'd

9. Conduct regular, as-issued access card inventories. This is the actual, physical account of all access cards. Where/when an access card cannot be physically accounted for, same should be voided immediately. These inventories should be conducted **at least** once every year and more frequently if there have been any unexplained losses. Only give 24-hour access to employees who truly need it as part of their job function. Lost, missing, or stolen cards, especially those with 24-hour access, is a definite security liability. Establish a protocol for the after hours reporting (and quick voiding) of lost, missing, or stolen cards and cards belonging to employees terminated after regular business hours.

Awareness and Education

This is an extremely important, and often overlooked, factor. Vigilant staff can greatly help improve the overall security level by:

1. **Safely** challenging strangers. This can include:
 - a. Persons wearing clothing inconsistent with the company dress code.
 - b. Persons who's grooming and hygiene is not consistent with the corporate environment.
 - c. Persons the employees have not seen before and/or not wearing not wearing visitors' badges.

More information on this topic is available in ***Intercon's Employee Procedures For Challenging Unknown Persons Document***

2. **Reporting** suspicious activity such as:
 - a. Doors propped open.
 - b. Locks taped open.
 - c. Persons loitering near access-controlled doors.
 - d. Computer equipment left beside doors, and so on.

More information on this topic is available in ***Intercon's Definition of Suspicious Activity Document*** Same can be modified to fit your site and corporate culture. The above-noted, and other laptop/PC security topics, should be discussed at staff meetings. Consider the use of a Police Crime Prevention Officer or a Security Manager at some of these meetings. Circulation of computer security 'tips' or 'bulletins' can also be used to increase awareness. In sensitive areas, signage may help alert employees and reduce losses (i.e., Do Not Leave Your Laptop Unattended, etc.).



Small Industrial/Commercial Premises

Overview

These units present a definite security challenge. They are often easily entered by breaking through glass and are often subjected to cyclical, re-victimization. In some cases, the same burglars will wait until the computers stolen in the previous attack have been replaced. This usually takes roughly 30 to 90 days, at which time these burglars will attack the same location again.

Signage

Landscaping should **not** conceal exterior, civic address (and/or company name) signage at these premises. This signage should also be mounted high enough so as to be visible over trucks. Lettering should be very large (i.e., eight to 12 inches in height) and be mounted on a contrasting-coloured background. Signage should also be illuminated at night. Back-lit signage is preferable. Where/when lighting the signage is not practical; consider the use of Scotchlite™ or other similar, fluorescent material. To assist the police and security responding to alarms at larger premises, number the doors. Alarm system zone descriptions should include these numbers. Erect signage to this effect above all pedestrian and overhead doors (i.e., Receiving Door #7, etc.).

Safe Rooms

A safe room for all hard drives may be a useful tactic at vulnerable facilities and/or premises where there have already been multiple thefts. Safe rooms are best built with slab-to-slab walls, constructed from poured concrete reinforced with metal, re-bar rods. If this type of construction is impractical, consider two layers of ¾-inch plywood with expanded metal mesh between them. Use screws, **not** nails, to attach the plywood to the studs on both sides. Studs should be located no more than 12 inches apart, versus the usual 16 inches. On the side of the room a burglar would see, cover the plywood with drywall. The fire-rated door to this room should be 45mm (1 ¾ inches) thick and constructed of sheet metal at least 1mm thick. This door should also open **outward**. Tests in Israel confirmed that this is more secure than inward-opening doors. Upper and lower, high quality, deadbolt locks are recommended here. These deadbolt locks should have 25mm (1-inch) bolt throws, anti-drill plates, cast or machined-beveled spinner washers, metal strike boxes, and high security keying. The Medeco™ model #11W0200-626-M2 (carried by Intercon) is highly desirable for these applications. As well, the door's exterior handle should only be glued on or held on by one or two, very small screws. This is so that it will come off in the burglar's hands if they apply force to the handle when the door is locked. 'Spider' locking systems, with four or more locking arms, are an even more secure alternative here.



Small Industrial/Commercial Premises cont'd

Safes

Underwriters' Laboratories of Canada (ULC)-rated money safes may be installed here as an alternative to a safe room. Employees should be instructed to place their laptops in the safe at the end of their business day. The last employee to depart should close the safe, lock it, and set the alarm system. Safes should be located in a public area if at all possible. Ideally, they should be visible to a Police/Security Officer sitting in his/her patrol car. Only ULC 'B-rated' money safes, or safes with a higher rating, are acceptable for this application. ULC 'B-rated' money safes have ½-inch thick steel doors and ¼-inch thick steel walls. If the safe weighs less than 750 pounds, it should be bolted to the floor. Safe combinations should be changed whenever a combination holder leaves the company's employment. Fireproof safes offer minimal protection from forced entry and are **not** suitable for this application.

Alarm Systems

Intrusion detection alarm systems are definitely recommended for premises containing numerous PC's and laptops. Laptop and PC thieves will often attack either the phone line and/or the alarm system. For this reason, these alarm systems should incorporate the following features:

1. A phone line protection system, which treats an attack on the phone line in the same manner as an attack on the protected property. In the event of an alarm, a central monitoring station would send Security Officers and/or the police to the site to investigate. DVAC phone lines are preferred in this regard due to continual 'polling' (i.e., every three to five milliseconds). This is done via a DVAC module, which is basically a modem. Dialer-type alarm systems should **not** be utilized at these premises. Cutting a phone line connected to one of these systems would **not** result in an alarm until six to 24 hours **after** the line was cut. Furthermore, in most cases, it would only be a local alarm. Where/when DVAC or TCP/IP technology with 'polling' is **not** available; your system should be equipped with cellular back up. The cellular back up should be located in a secure area that is separate from the primary alarm system.
2. Purchase only ULC-listed control units with built in tamper switches.
3. Locate the control unit in a secure closet with a deadbolt lock. (**Note: Please see our door specifications listed on Page 8, Item #2**). The deadbolt lock should have a 1-inch bolt throw and a metal strike box.
4. To detect sabotage, ensure that **all** devices have tamper switches, which are monitored 24-hours-a-day, and/or have end-of-the-line resistors. To prevent the deliberate blocking (i.e., 'masking') of motion sensors, purchase only motion sensors with anti-masking technology.
5. To prevent sabotage/blocking off of the motion sensors, mount them as high as possible. In some instances, overhead, ceiling-mounted, motion sensors may give the best coverage with the lowest potential for sabotage.



Small Industrial/Commercial Premises cont'd

Alarm Systems cont'd

6. Where possible/practical, use only concealed contact switches.
7. Rooms/areas with significant numbers of PC's and laptops should have alarm systems that meet the ULC, Level 2 extent of protection standard. In general terms, this means that **all** points of entry are alarmed and that there is also interior space protection.
8. Doors 10 feet wide, or wider, require contact switches at **both** ends. This is because it is possible to pry these doors open at one end and not activate the alarm switches at the other end.
9. To determine if a burglar has/has not accessed computers in sensitive areas, install additional, strategically-located internal alarm devices, which will help create a record of his/her movements. During a burglary, alarms from the detectors can allow the central monitoring station to 'track' the suspect's movements and relay same to responding police or security units.
10. Most motion sensors come with a pre-wired, red, LED indicator that lights up when movement in a protected area is detected. Since these lights can be used to determine areas of coverage, and/or the rate of movement required to cause an alarm, we recommend disconnecting the indicator light or purchasing motion sensors with no indicator light.

Alarm System Response

Some clients will rely only on police response to their alarm systems. Our concern with this is that responding police have **no** keys, and will **not** accept them, and cannot always determine if the premises has been entered. This is especially true where/when the entry may have been via an adjoining unit or possibly a roof, which cannot be accessed without a ladder. Even if there are no outward signs of forced entry, the premises should be entered by a trained Operative with keys. Keys should be kept in secure custody, such as a numbered envelope, and stored in a locked key box until the Operative arrives at the alarm scene. Keys are best protected when the Operative does not receive the key envelope number until they arrive at the premises with the activated alarm system. In addition to a thorough, internal examination, Operatives with keys will leave a written report outlining their findings. To protect client confidentiality, this report would be enclosed in a sealed envelope and/or left in a secure location.



Small Industrial/Commercial Premises cont'd

Roof Protection

Enterprising thieves, wishing to avoid detection by an alarm system, may attempt entry via the roof, especially where same is 16 feet or less above grade. To reduced the potential for roof attack, please make note of the following:

1. Do not store ladders outside.
2. Do not store tall piles of skids, dumpsters, vehicles, or any other climbing aid, within 10 feet of the building.
3. Trim tree branches, if they are two inches or thicker, within 14 feet of the building.
4. Cover climbable gas or drain pipes with sheet metal. Install lockable, expanded metal mesh 'cages' over built-in ladders.
5. Ensure roof hatches have padlocks, ideally two, and roof doors should have deadbolt locks, strike cover plates, and non-removable hinge pins where the door opens outward.
6. Install alarm contact switches on roof doors, hatches, and the covers for built-in ladders. Consider under-the-roof, indoor motion sensors or truss-mounted, weight sensors where roof access seems logical. For example, at the top of a built-in ladder or where a burglar would step from a nearby tree or gas pipe onto the roof.

Vehicle Attack

These types of premises can be vulnerable to a drive-in-type, vehicle attack. Grade level planters, concrete highway safety barriers, large landscaping rocks, or bollards (specifications available from an Intercon Account Executive) are the best counter-measures. They should be deployed in front of all grade level, vehicle-accessible, points of entry and be spaced no more than 40 inches (one metre) apart. A U-shaped configuration is recommended for high-traffic areas. Mechanical bollards, which can be remotely raised and lowered as required, should be considered for locations where the installation of permanent planters, landscaping rocks, etc. is not practical. However, mechanical bollards are very expensive at \$15,000.00 U.S. per set plus cabling and installation costs. (**Note:** *Hydraulic bollards are **not** recommended in cold, winter weather climates*). As a low cost alternative to bollards, planters etc., consider the regular use of 'blocker' vehicles at the end of the business day. Grade level, overhead doors, especially those constructed from ¼-inch plywood, are particularly vulnerable. Floor-mounted, removable bollards installed **inside** of the overhead doors are recommended here. As noted above, these bollards should be spaced no more than 40 inches (one metre) apart and should be located no more than 12 inches from the door(s).



Security Devices

As previously stated, in our view, a layered, multi-faceted approach incorporating access control, target hardening, and a wide range of other security tactics are necessary to properly protect laptops and PC's. The RCMP also recommends a similar approach. **Part** of that approach at some locations may be so called 'point protection' on individual laptops and PC's. The following is a list of PC and laptop security products we have encountered. (**Note: This list should not be regarded as complete or as an endorsement or recommendation of any of the products listed**).

Sonic/Local Alarms

These units work on the same principle as car alarms and are usually activated by a key. Makers, and users, assume that the noise will attract attention and deter a thief. In our view, their value in isolated or 'lonely' environments is limited. Available products include:

1. **bluVenom™**: This is a two-stage alarm unit that locks into the floppy drive or parallel port with a coded key. Minor/initial movement results in a short duration warning 'hiss'. If movement continues, a 120-decibel siren is activated.

Contact: www.lh-group.fi/alarms.htm

2. **Wobbler™**: An alarm 'card' is installed in one of a PC's spare expansion slots. Movement of the PC, with the unit turned on, results in a 110-decibel siren.

Contact: www.aztec-coverpro.com

3. **SonicLock®**: This externally-attached unit fastens to your carrying case, or to the laptop security slot via an adaptor.

Contact: www.kensington.com

Tracing/Stealth Software

Basically, this software communicates with a 24-hour, central monitoring station. This software primarily 'calls home' either at a specified time of day, on boot-up, or when a password is not provided. This facilitates the use of non-broadband Internet connections, which are **not** always 'on'. It advises the central monitoring station of the phone number it is calling from. When the laptop or PC is reported stolen, this information is used to locate same. Products/suppliers include:

1. **Computrace®Plus**: By Absolute Software Corp.

Contact: www.absolute.com

2. **LapTrak™**: From Secure-It.

Contact: www.Secure-It.com (or www.kablit.net)

3. **StealthSignal**: From Security Products, Inc.

Contact: www.computersecurity.com



Security Devices cont'd

Marking/Labeling

These products facilitate the labeling of computer equipment with a company name or logo and/or a registration number. In some cases, the numbers are recorded and/or listed in a registration database. Suppliers/products available include:

1. **MARKITWISE:** Supplies a wide variety of security marking labels, seals, and marking pens including ultra-violet markers.

Contact: www.markitwise.co.uk

2. **Make Your Mark™:** For about \$30.00 (and up) per piece, items are labeled with your company logo, given an identification number, and registered in a database. Window decals are also included.

Contact: www.makeyourmark.net

3. **S.T.O.P. Asset Tracking:** From Security Products, Inc. Consists of tamper-proof, metal plates with bar codes and indelible equipment tattoos.

Contact: www.computersecurity.com

4. **Police Marking Systems - Operation Provident:** A nationally recognized Canadian numbering system provided and administered by your local police department. Your business will be issued a unique Operation Provident number, which would then be engraved on all expensive computers or other electronic equipment. Posting a warning sign at your business will caution thieves that your expensive equipment is marked and identifiable. This will deter thieves and aid in the return of recovered assets. Contact your local police department for more information.

Cable Locks

Generally speaking, cable locks are used to attach laptops, and sometimes other equipment, to difficult-to-move objects (e.g., desks, pillars, etc.). It should be noted that cable locks are effective protection against opportunistic theft **only** where/when lots of witnesses are present. Prepared and determined thieves, where/when there are no witnesses present, can cut cable locks. Some laptops only have a plastic hook/hasp that the cable attaches to. This means that the cable and hook can be easily pulled off the laptop's outer casing. The preferred type of hook/hasp is made of metal, which is integrated into the laptop's metal frame. Suppliers of cable locks include:

1. **AnchorPad®.**

Contact: www.anchorpad.com

2. **Computer Security Products, Inc.**

Contact: www.computersecurity.com



Security Devices cont'd

Cable Locks cont'd

3. **Kensington Technology Group (Division of ACCO Brands, Inc.).**

Contact: www.kensington.com

4. **SecurTech Co. International.**

Contact: www.securtech.com

Biometric Fingerprint Authenticators

These devices may deter theft by making the laptop or PC unusable to anyone but the owner/designated user. Products/suppliers include:

1. **Targus DEFCON Authenticator™:** From Targus.

Contact: www.targus.com

2. **U-Match® Mouse:** From Secure-It.

Contact: www.Secure-It.com (or www.kablit.net)

(Note: When traveling with a so-equipped laptop, keep the fingerprint authenticator in a separate case. This makes it even more difficult for the thief because he/she will not know what type of device they have to defeat).

Enclosure Locks (Cages)

In our view, these are the best products for securing PC's located in vulnerable areas. Suppliers include:

1. **Metalex.**

Contact: www.metalexproducts.com

2. **AnchorPad®.**

Contact: www.anchorpad.com

3. **Secure-It.**

Contact: www.Secure-It.com (or www.kablit.net)

*(Note: Caseva Security Products, **contact: www.caseva.com**, also offers a desktop enclosure lock for laptop computers).*



Security Devices cont'd

Secure Laptop Docking Stations

The best product, for laptops left in unattended offices for long periods, is a secure docking station. The docking station should be installed on a roller tray, which can be rolled into lockable, reinforced furniture. One supplier is:

1. **AnchorPad®.**

Contact: www.anchorpad.com

Plate Locks

In our view, plate locks are the second best way, after secure docking stations, to protect laptops. These locks are also very effective for hard drives. Plate locks typically consist of a plate, which is secured to the laptop or hard drive with **very** strong glue and, a second plated bolted and/or glued to a piece of furniture. They do not allow the protected item to be moved around the work area. Plate locks are available from:

1. **AnchorPad®.**

Contact: www.anchorpad.com

2. **Computer Security Products, Inc.**

Contact: www.computersecurity.com

Drive Locks

These units lock out unauthorized disks and/or prevent unauthorized disk removal. One supplier of such products is:

1. **AnchorPad®.**

Contact: www.anchorpad.com

Electronic Article Surveillance (EAS)

These systems are very similar to store anti-theft systems. Sensor strips are attached to computer equipment with a **very** strong adhesive. When a protected piece of equipment moves past a 'detection arch', a local siren, horn, or chime is activated and in some cases, a security console may receive an alarm. These systems can also be also interfaced to certain access control systems. If a protected piece of equipment is moved past a sensor, there will be no alarm if the access card of the person the equipment is assigned to, is also present. A supplier of EAS for laptops and PC's is:

1. **IBM:** A chip is imbedded in the laptop during the manufacturing process.

Contact: www.can.ibm.com



Encryption

Sensitive corporate, or personal, data should be encrypted. Central repositories, such as databases (e.g., Oracle, IBM DB2, Microsoft SQL Server, etc.), usually have a built-in encryption feature. Any access to the data is strictly controlled on a 'need-to-know' basis and every access is logged.

Many companies are resorting to the implementation of so-called 'thin clients'. This is whereby the individual workstations are running and accessing everything from the servers. Therefore, there is no need for the hard drives. Should any such workstation be stolen, it will prove to be totally useless.

These days, from an intelligence gatherer's perspective, it is not as much the physical theft of a hard drive or workstation that is the major problem. It is the attack on the network itself that will usually yield the biggest pay-off to the professional intelligence gatherer. A skillful attacker may steal the sensitive information with great impunity, from the relative safety of his/her own home; there is no need to expose oneself through a burglary attempt.

Another potential security problem is caused by how most operating systems delete files. When you encrypt a file and then delete the original plaintext file, the operating system does not actually physically erase the data. It merely marks those disk blocks as deleted, allowing the space to be reused later. It is sort of like discarding sensitive paper documents in the recycling bin instead of the paper shredder. The disk blocks still contain the original sensitive data you wanted to erase, and will probably be overwritten by new data at some point in the future. If an attacker reads these deleted disk blocks soon after they have been de-allocated, he/she could recover your plaintext.

The only way to prevent the plaintext from reappearing is to somehow cause the deleted plaintext files to be overwritten. Unless you know for sure that all the deleted disk blocks will soon be reused, you must take positive steps to overwrite the plaintext file, and also any fragments of it on the disk left by your word processor.

More modern operating systems sometimes use what is called a 'journaling filesystem'. This takes the temp file problem you might find in a word processor to the next level by making a second copy of every single item written to the filesystem, which then gets stored in a private filesystem area. This journal of 'disk writes' serves as a map for everything that has changed on the disk over time and allows the filesystem to recover more easily from damage. The NTFS filesystem on Windows NT/2000/XP is an example of such a filesystem. Mac OS X 10.2.2 also has a 'journaling extension' for HFS filesystems.



Encryption cont'd

Another kind of attack that has been used by well-equipped opponents involves the remote detection of the electromagnetic signals from your computer. This expensive and somewhat labour-intensive attack is probably still cheaper than direct cryptanalytic attacks. An appropriately-instrumented van can park near your office and remotely pick up all of your keystrokes and messages displayed on your computer video screen. This would compromise all of your passwords, messages, and so on. This attack can be thwarted by properly shielding all of your computer equipment and network cabling so that it does not emit these signals. Some government agencies and defence contractors use this shielding technology, known as 'Tempest'. There are hardware vendors who supply Tempest shielding commercially. Laptop computers with LCD displays produce no video emissions.

Virtual memory allows you to run huge programs on your computer that are bigger than the space available in your computer's semiconductor memory chips. This is handy because software has become more and more 'bloated' since graphical user interfaces became the norm and users started running several large applications at the same time. The operating system uses the hard disk to store portions of your software that are not being used at the moment. This means that the operating system might, without your knowledge, write out to disk some things that you thought were kept only in main memory; things like keys, pass-phrases, and decrypted plaintext.

This swap file can be accessed by anyone who can get physical access to your computer. If you are concerned about this problem, you may be able to solve it by obtaining special software that overwrites your swap file. Another possible cure is to turn off your operating system's virtual memory feature. Microsoft Windows allows this, and so does the Mac OS. Turning off virtual memory may mean that you need to have more physical RAM chips installed in order to fit everything in RAM.

There are many stand-alone encryption tools on the market. One of the best ones comes from the PGP Corporation (head office Palo Alto, CA, **contact: www.pgp.com**). PGP comes in three flavours: Personal, Workgroup, and Enterprise.

Some newer versions of PGP (after Version 6.0) can display decrypted plaintext using a specially designed font that may have reduced levels of radio frequency emissions from your computer's video screen. This may make it harder for the signals to be remotely detected. This special font is available in some versions of PGP that support the 'secure viewer' feature.

(Note: Laptop computers with LCD displays have no need for this special font because they produce no video emissions).

PGP is a tool for keeping the data safe. It has three main components:

1. PGPkeys: Create the personal keypair (a private key and a public key) and get and manage the public keys of other people.
2. PGPmail: Encrypt e-mail messages to other people and decrypt e-mail messages sent to you.



Encryption cont'd

3. PGPdisk: Encrypt a portion of a hard disk so that it is fully protected even if it is stolen.

PGP also does things like secure ICQ communications, wipe files so that they are completely gone, and create self-decrypting archives.

PGPdisk is an easy-to-use encryption application that enables you to set aside an area of disk space for storing your sensitive data. This reserved space is used to create a file called a PGPdisk volume. Although it is a single file, a PGPdisk volume acts very much like a hard disk in that it provides storage space for your files and applications. You can think of it like a floppy disk or an external hard disk.

To use the applications and files stored in the volume, you mount it or make it accessible to you. When a PGPdisk volume is mounted, it may be used as any other disk. You can install applications within the volume or move or save your files to the volume. When the volume is unmounted, it is inaccessible to anyone who does not know your secret pass-phrase. Even a mounted volume is protected; it is stored in encrypted format unless a file or application is in use. If your computer should crash while a volume is mounted, the volume's contents remain encrypted.

Travelling with Your Laptop

1. Write your name and company name on the battery and/or place your business card inside the battery compartment.
2. Consider the use of a laptop alarm. Some are triggered only by movement of the laptop (not too practical when traveling), or by moving the laptop a certain distance from the owner (preferable), or by a signal from the owner when they notice the laptop is missing. Their effectiveness is similar to audible car alarms and they should **only** be used in addition to other precautions.
3. Do **not** travel with your laptop in a purpose-built, laptop bag with the manufacturer's colour scheme, logo, or name on it. A distinctive or colourful sports bag or briefcase is preferable. The distinctive colouring is to assist the police in the event your laptop is stolen in a public area. For example, at a busy airport, the police are unlikely to stop every person, meeting the description of the thief, who is carrying a black briefcase. Whatever bag/briefcase you choose, same should be lockable.
4. **Never** leave laptops visible in unattended vehicles, even if the doors are all locked. Locked in the trunk is the preferred location.
5. Do **not** rent cars that have a passenger compartment, trunk release, which cannot be locked with a key.
6. When using cabs or shuttle buses, keep your laptop with you at all times.



Travelling with Your Laptop cont'd

7. Be alert/watch for:
 - a. Distraction thefts at airports (e.g., when in the ticket/check-in line, when going through metal detector screening areas, etc.).
 - b. Persons carrying coats over their arms, which can be used as a vision block. Pay special attention to these persons if the weather does not justify the use of a coat (e.g., not raining, **very** hot day, etc.).
8. Be alert for persons who:
 - a. Request the time.
 - b. Request you to make change.
 - c. Spill something on you.
 - d. Advise you that you have dropped something.
 - e. Create 'fights' or 'arguments'.

All of these are distractions designed to get you to look away, or distance yourself, from your laptop (and/or other items of value).
9. Your laptop should never be out of your sight. In general, it should be with you or locked up and/or hidden.
10. Travel with a cable lock or chain and padlock and use it.
11. When using public washrooms, take your laptop into the cubicle. Remain alert for possible 'reach over/reach under' theft. Where available, consider locking your laptop in a locker **before** using the washroom.
12. To minimize the potential for a 'grab and go' theft, wash your hands using the sink most distant from the door and keep your laptop in front of, or between your ankles/feet.
13. When using a pay phone, hold onto your laptop's carrying strap.
14. If you tend to fall asleep in public places (e.g., on the bus, train, plane, etc.) or if you concentrate on reading in public areas, use the laptop as a 'pillow' or 'book rest' and wrap the strap around your wrist, ankle, etc. Many laptops are stolen by perpetrators using the seat/bench/chair next to the victim.



Travelling with Your Laptop cont'd

15. Laptops are extremely vulnerable in hotels. Stay in hotels where the room doors are equipped with electronic access card readers and **not** keys. This is because the card reader will provide a forensic audit trail and this will discourage theft by hotel employees. Ideally, stay in hotel rooms that have windows that are **not** accessible from the ground, a balcony, or the roof. From a thief's perspective, rooms closest to the stairwells are the most desirable. When checking in, do **not** let bellhops put your laptop onto a luggage cart, which they may leave unattended. When leaving your laptop in your unoccupied room, re-pack same, along with all of the peripherals, so that the hotel staff does not know it is there. Lock all luggage to make it more difficult for a burglar to find what he/she is looking for. If your room is equipped with a safe, and your laptop will fit, store it in same. Where/when you feel your laptop is at risk in your unoccupied room, ask the hotel front desk staff if you can store it in their safe. If this acceptable to them, get a receipt. Where/when you do not have time to put your laptop away, use your cable lock.
16. Laptops are especially vulnerable during conferences, most often during set-up and break/lunch periods. While conducting presentations, do not leave your laptop in an unlocked, unoccupied conference room. Either take it with you or use your cable lock to secure it to an immovable, indestructible object (e.g., a desk, pillar, etc.). (**Note: Please also see Page 5, 'Identification' and Page 23, 'Travelling with Your Laptop'**). If organizing a conference or meeting where lots of laptops will be in use, consider utilizing a lockable laptop cart. (**Note: One supplier of such laptop/equipment carts is *AnchorPad*[®]. They can be contacted at www.anchorpad.com**). Another alternative is to use Security Officers to protect laptops left in unoccupied conference rooms.



**Intercon
Security**

THE LAPTOP & PC SECURITY GUIDEBOOK

Acknowledgments

Mike Fenton

Jill Brown

Emanuel P. Jech

Gerry Hegarty

Chris Jaynes

Robert Sombach

Robert Bellemo

Kevin Matthews

Taleen Merjanian

Andrew Young

Mark Drysdale

Terence Kilgore

Emanuel J. Jech

Dave Cook

The Royal Canadian Mounted Police (RCMP)

Peel Regional Police

The Law Enforcement Officer's Complete Crime Prevention Manual

Safeware® The Insurance Agency, Inc., Columbus, OH

PGP Corporation, Palo Alto, CA

This document is intended for the sole use of Intercon Security and its clients. No one is permitted to reproduce this document in any form, in whole or in part, without the permission of Intercon Security. © 2004 Intercon Security.

40714