Protecting assets at UBC

We normally find that UBC has a small proportion of individuals who are on campus expressly for the purpose of theft of property. We call them “motivated offenders”. When you have:

1. A motivated offender;
2. Target property. At UBC, in most cases, the exposed assets are cash, drugs, or desirable and easily-fenced electronics (most typically Apple computers, digital cameras, projectors, etc); and
3. The opportunity to steal the property without getting caught.

We have what we call the ‘tripod of opportunistic crime’.

We call it a tripod because if you take away any one of these elements the tripod will not stand. In reality, it’s impossible to remove the offenders and usually very impractical to completely isolate or protect the property, so we focus our efforts on reducing the last element, the opportunity to steal the property without getting caught.

There are two main elements at play in this strategy: denying easy observation (‘casing’) of these assets to the offenders and increasing the difficulty (or risk of being caught) involved in attempting to steal them.

At UBC we focus on the prevention of tampering or break-ins at exterior doors and windows, interior corridors, access points to offices, laboratory areas, or storage facilities. We want to reduce the likelihood that unauthorized people will be able to gain access to our protected assets---or if they do, that authorities will be alerted and can respond.

1. The perimeter of a building or workspace is our first line of defence. Exterior building envelopes and interconnections between buildings should present a high-security profile to reduce opportunities for unauthorized access into the building or area.

   Unauthorized access through doors or windows to the interior of a building or workspace can allow suspects to work unobserved to gain access to assets within the facility. Once inside, they can and will use any amount of force necessary to get at the target property, often causing serious damage that can be very costly to repair.

   This means that highly effective doors, windows and locking systems must be in place and maintained properly; it also means that the locked condition of these access points must be confirmed when the building closes for normal business functions, effectively whenever it becomes unpopulated by staff.

   Lockup is typically done by custodial workers who should check all doors, including communicating stairwells, when locking a facility. Care should also be taken to ensure doors are not blocked open for convenience during custodial working hours.

2. It is essential to train staff to challenge strangers and report any suspicious circumstances or individuals in or around the facility to Campus Security. Often students may be the only building occupants; they should also take responsibility for observing and reporting unusual occurrences.

   This also involves consideration of mixed user groups, the length of open hours, whether strangers are readily identifiable, and are always identified by staff in the area, etc.

3. Desirable consumer grade computer equipment (particularly Apple or Mac equipment) is well known to be selectively targeted in institutional break & enters; this elevated risk can be mitigated in part by minimizing the opportunity for casual observation of the high-value equipment and effectively hardening access points against unauthorized entry by installing electronic security systems to alert Campus Security to unauthorized access and using devices such as locks & restraints to increase the difficulty of removing the equipment.