Business Security Guide

Protecting your assets and avoiding losses

26/11/2012
Halkyn Consulting Ltd
Taz Wake, Security Director

Securing your business – reducing the risk of burglary and robbery

Robust security is crucial for the success of businesses of any size. However, small firms face particular issues when they seek to strengthen their security position. Typically, a small business's budget won't run to hiring a dedicated security staff or state-of-the art security hardware.

It's all the more important, therefore, for small firms to be smart about security. This document will discuss approaches to minimising the risks, focussing on two potentially serious risks to small business – robbery and burglary.

As part of our commitment to improving security awareness, reducing crime and protecting assets, Halkyn Consulting's security team has put together this document to help small – medium businesses get a better understanding of what risks they face and how best to manage them.

We have also included two easy to follow Risk Assessment Guides to help give an idea of what areas of concern might be most applicable. Both guides are there to help inform decisions and should never be used in place of expert advice. If you have any doubts about your security or would simply like to find out a bit more about what you can do to help prevent crime, then visit www.halkynconsulting.co.uk and get in touch with our security professionals.

What is a robbery and what is a burglary

Both robberies and burglaries will take assets from your company, cost you money and leave you feeling victimised, but they are different enough that you need to consider them separately.

To keep things simple, when we talk about a robbery in this document, we mean the situation whereby a hostile person, or group of people, comes into your business to steal property, assets or valuables during the business day[1].

A burglary is the same situation but taking place when the premises are unoccupied – normally overnight or during holiday periods[2].

Who gets robbed?

There is an idea that robberies only take place in banks and jewellery stores, but the reality is very different. All kinds of business can be robbed, and robbers will often try to take personal items from staff and customers, not just business property. While robbery is quite rightly reported as a violent crime, there is some good news in that it is still quite rare.

[1] For UK readers, Section 8 of the Theft Act 1968 states: "A person is guilty of robbery if he steals, and immediately before or at the time of doing so, and in order to do so, he uses force on any person or puts or seeks to put any person in fear of being then and there subjected to force."

[2] Again, for UK readers Section 9 of the Theft Act 1968 states: A person is guilty of burglary if: (a)he enters any building or part of a building as a trespasser and with intent to commit any such offence as is mentioned in subsection (2) below; or (b)having entered any building or part of a building as a trespasser he steals or attempts to steal anything in the building or that part of it or inflicts or attempts to inflict on any person therein any grievous bodily harm.

In the UK, in the year ending June 2012, there were over 71,000 reported robberies[3], which is around 2% of all police recorded crime and the incidents are very heavily centred on urban areas (half the robberies were in London, and another 15% in Manchester & the West Midlands).

Unlike robberies, burglaries are rarely "violent" offences in that they predominantly take place when the premises are unoccupied; however they are much more common. In the UK, for the year ending June 2012, there were over 480,000 offences reported to the police (the British Crime Survey reported 677,000 incidents in the same period)[4]. Of the incidents reported to the police, slightly more than 50% were "non-residential", including commercial property, warehouses, storage facilities etc.

So, in very general terms, if you have anything of value – including customers – then you may well be at risk from a robbery or a burglary. If your offices or storage facilities are in a metropolitan area, or even near to a big city, then the probability that someone will try to steal from you increases.

However, there is nothing inevitable about crime.

Criminals, generally, look for the path of least resistance and by implementing some simple, good practice, security controls; you can make your business premises unattractive enough that they will go elsewhere. This doesn't require you install Fort Knox style guards and fences – apart from anything else, good security should never cost more than what it is protecting – but it does mean you should give some genuine consideration to your risks and security measures.

Reducing the risks, protecting your business

The key to ensuring that your security is appropriate, effective and within budget is making sure you take a sensible approach. One of the best known approaches is to follow the Plan-Do-Check-Act (PCDA) methodology.

Like all security, this is an iterative process and you should be constantly cycling through it to see if you can get improvements. To assist, we have broken down what you should be considering at each stage:

Plan

Before you do anything build a clear-cut plan of action. No matter how many times you go through the cycle, the planning stage should always be the most important and will often be the longest & hardest to complete.

You need to look at your business in detail and sensibly identify what valuables you have and how important they are to you.

Your first concern has to be protecting life and limb. Nothing is more important than your own physical safety and the physical safety of your family, employees and customers. After protecting people, your next concern should be for protecting the assets that are most important to your business's survival. **These may not be your most valuable assets in cash terms**.

[3] Data from http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/period-ending-june-2012/stb-crime-in-england-and-wales--year-ending-june-2012.html#tab-Robbery (accessed 23 Nov 12).

[4] Data from: http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/period-ending-june-2012/stb-crime-in-england-and-wales--year-ending-june-2012.html#tab-Burglary (accessed 23 Nov 12).

Plan – Risk Assess

If this is the first time you have given your business risks serious consideration, you can use the Risk Assessment Guides in this booklet to help steer your planning – after you have been through the process a few times, you may well have your own material which is more specific and more accurate.

Plan – Security Controls

Once you have identified your areas of risk, you need to consider what measures you can take to reduce the probability or impact, should you become a victim of crime. Basic crime prevention measures for burglaries and robberies are included in this document and should be viewed as a way of reducing the probability. If you need to reduce the impact of crime you need to consider insurance to protect against financial loss[5] and consider having spare equipment at alternate sites to prevent service loss.

Plan – How to respond

As part of your planning phase, you need to also prepare instructions for your employees on what to do should the controls fail and your business becomes a victim of crime. Remember, robberies and burglaries are stressful so your guidance to employees should always be simple and easy to follow, and always available to them – there is no point having it stored on your IT equipment when that has been stolen.

As part of the advice you give your employees, keep in mind the goal of preventing harm to them. **Never** expect your staff to physically challenge intruders and **never** instruct them to risk their own safety protecting property. Things can always be replaced, but people cant.

Do

Once your planning is completed you need to put your plans into action.

This is the stage in the cycle where you implement any new security controls you have decided upon (for example, new locks, or new CCTV) and if you have planned properly this should be a straightforward activity.

Where possible you should try to ensure your implementation plan complements existing security controls and doesn't create a period of time where you are more vulnerable to crime. For example, if you are replacing window locks, make sure that the new ones are fitted as soon as the old ones are removed rather than allowing all the old ones to be removed before the new ones are fitted as this will invariably create a period of time where no locks are in place.

Make sure you keep good documentation around the changes you make in this stage, especially if any tactical decisions are required which deviate from the original plan.

Check

Once your new security controls are implemented set up a process which checks the efficiency and effectiveness at set intervals.

[5] If your business deals with customers, you need to be aware that most insurance policies don't provide any coverage over the loss of business that comes from customers losing confidence in your ability to provide a safe environment for them. Insurance is a supplement to good security, not a replacement for it.

The exact timescales will vary depending on your business size & needs, but in general you should consider having a way to review things at least every six months to allow you to verify that the controls you have brought in match your plan.

If you are in a low crime area, this check process might involve an annual review of the security controls to make sure everything is working, while businesses in high crime environments may need more frequent checks.

You don't need to only look at burglary and robberies here – if your risk assessments are in place you can monitor the effects your security has on all forms of crime, such as shoplifting, employee theft etc.

Act

Once your checking process identifies a problem – for example, you might have put in electronic security locks that are malfunctioning, or the crime rates in your area have significantly changed – you need to begin the process of working out corrective actions.

This doesn't always mean you need to keep spending more money, adding controls, in a never ending cycle. Frequently you will find that a control you have in place is no longer cost effective and you should cease to use it, freeing up resources for other activities – or better security controls.

Once the trends in the check stage have triggered action, you need to look into the root cause of what has happened to determine the best solution. Once you have this information, it is time to go back to the beginning and plan your changes.

What else?

No security is 100% effective, but going through this process and carrying out a proper risk assessment should give you the best chances of deterring criminals, defending against the ones who aren't put off and detecting the ones who get through your defences.

You should always work closely with other businesses in your community to help drive down crime across the board and maintain good relationships with your local police force to get up to date information on crime rates and the risks.

Crime Prevention & Response Advice

Here are some good practice tips on measures you can take to reduce the chance that you will become a victim of crime and, if the worst happens and you are, what you should do.

Robbery

Risks to

- Physical safety of people
- Goods and cash
- Valuable items or assets

How to prevent it

- Make sure that you have good lighting, both inside and outside the building, especially near cash registers or valuable goods.
- Eliminate external areas that could be hiding places.
- Restrict the number of entrances to the premises at night.
- Keep cash registers in prominent places
- Limit the amounts of cash on your premises. Use drop safes and take money to the bank on a frequent but irregular basis.
- Advertise that limited amounts of money are on the premises and that employees don't have access to safes.
- Install closed-circuit television cameras if the risk merits it.
- Train staff in robbery prevention and response.

What to do if it happens

- Train staff in robbery response so they know how to act to prevent escalation
- Do nothing to upset a robber
- Avoid startling a robber. If an event may startle him, give him warning.
- Cooperate. Hand over money or goods. Do not resist or give chase.
- In the face of threatened serious physical harm, fight back using anything at your disposal.
- Concentrate on memorising the details of the robbery for your police report.
- Particularly focus on memorising the robber's appearance, clothing, height, weight, voice, gait, etc.
- Record any details such as car registration number.
- Try to preserve forensic evidence, such as fingerprints by avoiding contact with surfaces that the robber may have touched. Stop others entering the premise or touching surfaces.

Burglary

Risks to

- Goods and cash
- Valuable assets
- Physical integrity of premises

How to prevent it

- Make sure that you have good lighting, both inside and outside the building, especially near cash registers or valuable goods.
- Eliminate external areas that could be hiding places.
- Restrict the number of entrances to the premises at night.
- Secure valuable items out of hours.
- Have obvious security controls – such as burglar alarms – and warning notices in prominent places.
- Ensure there is a well-understood process for making sure the building is secure at the end of the working day.
- Additional advice is provided in the checklist at the end of this booklet.

What to do if it happens

- Provide the police with the names and telephone numbers of employees that should be called if a burglary occurs. The designated employees respond to the burglary and assume responsibility for securing the building and assisting police in determining what has been stolen.
- If you discover a burglary and believe there is a chance the burglar may be inside, do not enter. Go elsewhere and call the police.
- Upon discovering a burglary, leave the scene intact until the police arrive.
- Do not open the business until the police have completed their investigation. Otherwise, valuable evidence may be destroyed by employees or customers.
- Be prepared to furnish the police with a list of stolen property, its description, serial numbers, and value.
- Cooperate with the investigation and prosecution by providing information as requested and testifying in court.

Risk Assessment Checklists

Understand your risks before you begin to implement controls

Business Security Checklist – Robbery Risk Assessment

Answering yes to the questions below indicates that the location is at a higher risk from robbery or there are security deficiencies that may encourage or enable robberies.

Assessment Area	YES	NO
Is your business a likely target for robbery?		
Is the business isolated from other businesses?	_____	_____
Does the business operate late at night?	_____	_____
Does the business deal with large amounts of cash after dark	_____	_____
Is the business known to keep large amounts of cash on hand?	_____	_____
Is cash transferred according to a set routine?	_____	_____
Is the business obviously operated by a single cashier?	_____	_____
Does the business have insufficient exterior lighting?	_____	_____
Can a robber approach your business without detection?		
Do posters and displays block visibility in and out?	_____	_____
Are there blind or hiding spots adjacent to the business?	_____	_____
Are there blind or hiding spots within the store?	_____	_____
Is the entrance close to the cash register?	_____	_____
Can a robber easily carry out a robbery in your business?		
Is the cash register within easy reach of the customers?	_____	_____
Are there blind or hiding spots near the cash register?	_____	_____
Are cash registers hidden from the site of other employees?	_____	_____
Is the safe or cash container easy to open?	_____	_____
Is the exit close to the cash register?	_____	_____
Do business doors open both ways?	_____	_____
Can a robber make a clean get away from your business?		
Is customer parking adjacent to a thoroughfare?	_____	_____
Are there blind spots in the parking area?	_____	_____
Can robbers "get away" with robbing your business?		
Are there no standard procedures for reporting crime to the police?	_____	_____
Are employees untrained in dealing with robberies?	_____	_____
Are cash totals not recorded regularly?	_____	_____
Can robbers be successfully prosecuted if arrested?		
Are you unwilling to participate in a trial or other legal proceeding?	_____	_____
Do you have no systematic procedures for maintaining evidence for police use?	_____	_____

Business Security Checklist – Burglary Risk Assessment

Answering yes to the questions below indicates that the location is at a higher risk from burglary or there are security deficiencies that may encourage or enable robberies.

Assessment Area	YES	NO
Is the business a likely target for burglary?		
Does the business lack perimeter protection?	_____	_____
Does the business store items of significant value?	_____	_____
Is the lighting of the business exterior inadequate?	_____	_____
Can the business be observed by burglars easily?		
Can a burglar approach the business without being observed from outside?	_____	_____
Is the cash drawer left closed after business hours?	_____	_____
Is the safe hidden from outside view?	_____	_____
Has the business decided not to use a burglar alarm system?	_____	_____
Is the business easy to break into?		
Are there unprotected openings larger than 96 square inches?	_____	_____
Can hinge pins be removed from exterior doors?	_____	_____
Are exterior easy to jimmy or pick?	_____	_____
Are locks and doors of poor quality?	_____	_____
Are locks and other security devices poorly maintained?	_____	_____
Is it easy to collect cash and high value items from inside the business?		
Are high value items accessible and not protected by security anchors?	_____	_____
Is cash stored in the business during non-operating hours?	_____	_____
Are cash and high value items not protected by an interior alarm system?	_____	_____
Is it easy for a burglar to leave the business with substantial amounts of "loot"?		
Is the parking lot poorly lit?	_____	_____
Are boxes, etc. allowed to collect near the fence or building?	_____	_____
Is there an exit leading to an alley or driveway?	_____	_____
Are some doors equipped with weak locks?	_____	_____
Can burglars be successfully prosecuted if arrested?		
Are you not willing to participate in a trial or other legal proceeding?	_____	_____
Do you have no systematic procedures for maintaining evidence for police use?	_____	_____

Burglary

Crime Reduction Advice – Prevention is better than treatment

Prevention Guide

The following guide details the areas you should consider to make your premises less attractive to burglars (deterrence) and harder to crack for those who are determined to get in (defend).

1. Fences and Gates

Fence the entire perimeter of the property, if your risk assessment identifies this as an area of weakness. You might need to reinforce the fence with barbed wire.

Avoid opaque barriers which will block your security view. If the appearance of the fence is important use a chain link fence with shrubs and bushes. Make sure that you keep important fields of view clear.

Secure gates with strong padlocks and chains when they aren't in use.

2. Parking Areas and Open Spaces

Secure ladders and storage containers at least 25m away from the building, to prevent intruders gaining access to roofs or upper level windows.

Put up signs in parking areas to remind customers and employees to lock their vehicles and not to leave valuable sin plain sight.

3. Exterior Lighting

Light your property. Do not depend on public street lighting or the lights from other properties.

Regularly inspect the lighting to ensure that it provides adequate visibility for the protection of customers and employees. Make sure that lighting does not cause glare to customers, employees or passing police patrols.

4. Doors

Don't use doors with panels or glass that can be kicked in or knocked out.

Make sure the frame is as strong as the door.

Reinforce any areas of structural weakness. For instance: install a metal lining on exterior wooden doors to resist drilling or sawing; secure double doors with heavy duty, multiple-point, long flush bolts.

All exterior doors should be constructed of steel, aluminium alloy, or solid-core hardwood – ideally constructed to meet ACPO guidelines such as PAS24 or EN14351.

5. Door Locks and Hardware

Exterior swinging doors should have a minimum one inch deadbolt lock, one inch throw bolt with a hardened insert, and free turning steel or brass tapered-cylinder guard.

Use steel strike plates on aluminium door frames. All outside hinges should have non-removable hinge pins.

6. Padlocks

The most common assaults on padlocks are made with bolt cutters or pry bars. To prevent this, padlocks should always be of the closed shackle type with a hardened steel lock case. You should also consider how the hinge holding the padlock is manufactured to prevent an attacker simply prying this off.

7. Windows

Windows should offer light, ventilation, and visibility, but not easy access. All windows which can open should be fitted with at least one lock. Locks should be designed so they cannot be reached and opened by breaking the glass.

Ground and first floor windows should be protected with burglar-resistant glass, bars, grilles, grates, or heavy-duty wire screening to provide optimum window security.

If your risk assessment supports it, fit laminated (at least 7.5mm grade) glass to windows.

8. Strong Room

Many businesses have or need a strong (or security) room to provide extra protection for valuable assets. If your business has such a requirement, the room should contain a door constructed of metal, with a robust deadbolt lock and the walls. Ceiling and floor should be reinforced with a secondary layer of material. Access to this room must be properly controlled.

Strong rooms should not be immediately obvious from outside the building and, where additional protection has been implemented, it should not visibly protrude beyond the main fabric.

9. Safes & Security Containers

Standing safes or strong boxes should be anchored to the floor or wall wherever possible. Cash amounts should be kept at a minimum by frequent banking. Never leave the combination written where it can be found.

Keep a complete list of serial numbers of all company equipment. When completed, lock the list in the safe and update it as needed.

Combinations should be changed on a regular basis (at least once a year) and must be changed whenever an employee who knows the combination leaves your employment. Records of every combination change (but not the combination) should be properly maintained.

10. Tools and Equipment

Unsecured tools or equipment may be stolen or used by a thief on your doors, safes, security room, cabinets, etc.

Tools and portable equipment should be secured in locked drawers or cabinets at the end of the business day and this should be built in to your end-of-work routines.

Business machines should be protected by installing appropriate locks which secure the equipment in place.

Blank cheques, credit card slips, and related machines and supplies should be locked in a safe or other security container when the business is closed.

11. Interior Lighting

Keep the interior of the business well lit. Burglars prefer darkened areas. Leave your blinds and drapes open and install locks on outside fuse boxes.

12. Alarms and Security Systems

Alarms can provide added protection to your business. However, installation of an alarm does not mean that other security measures are not necessary.

There are two basic types of intruder detection systems: audible and silent. The audible alarm typically sounds on the building while the silent alarm is monitored by a central station which notifies the police when the signal is activated.

Alarms should be professionally installed and you should ensure that you have a nominated key-holder who can be contacted at all times.

Alarm systems should contain a back-up, fail-safe system, a fire sensing capability, and a testing feature.

13. Key Control

Key control is an absolute necessity in all businesses. Master keys, safe keys, and others should be secured. A procedure should be established for issuing master or sensitive keys to employees on an as needed basis.

Where you use combination locks, or password protected systems, and copies are maintained, these should be sealed into an envelope and treated as a security key.

Spare keys should be kept in a known, secured, location and regularly mustered to ensure they are accounted for. Any locks that do not have spare keys should be replaced as soon as possible.

Where spare keys exist, the key in use should be rotated on a regular basis to ensure even wear and tear.