www.StyxSecurity.org

ISO 27001 Physical Security Toolkit

This is the "*say it like you mean it*" physical security toolkit for ISO 27001.

The criminal doesn't see your compliance, they see their opportunity.

These are the gaps in security, and your risks.

By thinking like the threat, we ask different questions.

Aimed at ISO 27001 consultants, this guide will help you *spot the gaps the criminals see*, and allow your clients to better understand their risks.

This is not a comprehensive guide to ISO27001's physical security standards and is intended for use by experienced information security consultants.

Enquiries@StyxSecurity.org

01924 654 130

Index

VIDEO GUIDES

This guide will be supported by audio / video commentary released over the coming weeks.

Click the image to go to the list of available guides.

Perimeters

How many perimeters do we have?
- Consider the boundary of each area as a perimeter with controls.
- Are the controls are varied, layered with increasing competency / diversity of skill to overcome, appropriate to the risk of breach?
- Can we detect attack, breach or transition between perimeters?
- Are sufficient layers in place with respect to the risk to the business?

What is the purpose of each perimeter with respect to the risk associated with each perimeter being breached?
- Protecting mobile assets like vehicles?
- Protecting sensitive information?
- Are we simply marking private property?
- Does the current state of the perimeter actually align with the intended purpose and threats to the business?
- Have needs changed since perimeter constructed?

Are there compromises to a secure perimeter?
- Shared access or right of way.
- Neighbours providing climbing aids or easy access.
- Emergency or fire regulations.
- Employee behaviour. *e.g. unofficial entrances, smoking, shortcuts.*
- Any furniture, etc providing concealment for breaches? *E.g. bike shelter up against fence provides both concealment and climbing aid.*
- How have we accounted for the above and controlled / accepted?
- Do we have to consider the building porous? See Main Entry.

Can we / should we detect perimeter breaches?
- Different sections of perimeter may have different risk of breaches depending on the approach. Open ground Vs good concealment.
- Is there an IDS or monitored CCTV providing alerts?
- If not, is detection realistically achievable without alert fatigue?
- Do we get sufficient delay after detection? What happens, who does it, is it tested and is it effective?
- What happens if a detection fails? What other opportunities are there?

What sensors / cameras are detectable from the outer perimeter?
- Which are visible and which are going to be a fun and rewarding surprise for an intruder? Any face-level CCTV to deter during recon?
- Are they a deterrent or information for an attacker?
- If facing more technical threats, how might an attacker use available technology to compromise perimeter sensors? *e.g. WiFi deauthers, IR.*

Perimeters

How is space classified between perimeters?

These are suggested categorisations.

Sterile – No entry by anyone, (can be anytime or at specific times).
E.g. between dual-layer perimeter fences, specific areas out of hours. Excellent for detection.

High security – Entry only by exception with authorisation and reason.
E.g. server rooms and adjacent power / comms.

Secure – Entry to specified employees with roles requiring access.
E.g. offices handling sensitive data.

Private – Areas not open to the public but not handing data or product.
E.g. staff kitchen, landing areas.

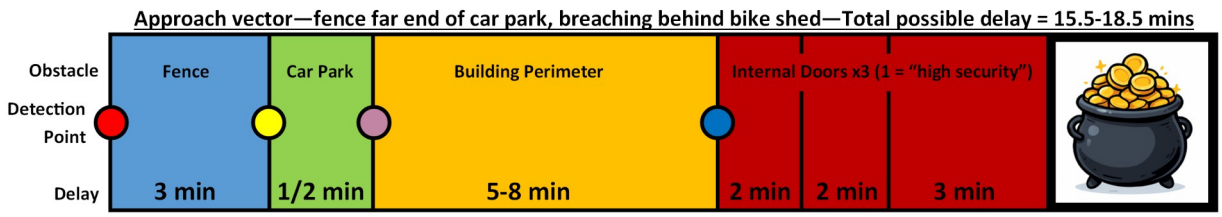
Public – Publicly accessible areas with no controls.
E.g. lobby areas.

Transitional – Areas which can be a mix, or divide zones.
E.g. Lobby, landing, delivery or screening areas.
Hard detection; perfect loitering places for threats.

Visualising Defences Vs Threats

We can use diagrams like the below to easily visualise and communicate the efficacy of our defences Vs the threats for various routes we think attackers would take. This diagram shows an imaginary attack at night, when the business is closed, breaching a fence at the far end of the car park. We can see how long it would take to breach all the layers we have (coloured boxes) and our detection opportunities (circles), e.g. PIRs, vibration sensors, etc.

This allows us to visualise our defences Vs risks to the business with respect to the delay after each detection point and our interdiction plan (guard response, police). We can then decide if controls are adequate, need enhancing or risk accepting.



Detection Points and Remaining Delay

- ~~Outer fence attack *15.5-18.5 min*~~
- Outer fence breach *12.5-15.5 min*
- Building attack *12-15 min*
- Internal door attack *7 mins*

Summary and points for exec review:

Guarding service response SLA = 12 minutes, 95% of the time.
Police response at 3-7 mins but historically contingent on confirmed breach (CCTV / guard).
Outer fence attack detection is not feasible. System has too many false positives—silenced.
Car park is sterile outside of working hours, therefore good detection opportunity with CCTV.
Must have good detection of attempted attack on building perimeter, not at breach.
If above not technically possible, consider internal delay systems.
Note no detection past first internal door—multiple alarms may illicit police response.

Controls

Are secure perimeters protected with adequate controls Vs our risk?

- What capabilities do our threats have?
- What is the risk presented by our various controls being breached?
- Have we considered changing tools and techniques available to different levels of threat? *E.g. simpler card cloning tech, Li-ion tools, relay attacks, bump keys.*
- Is there a diversity of skills / tools required to undermine / bypass multiple layers of security? Do some frustrate covert and some overt?
- Are controls resistant to insider collaboration? What additional physical controls might be required to reduce the risk?
- Are controls designed with consideration of human factors? *E.g. wedging doors open, shortcuts, tailgating, card passback.*
- Is lighting sufficient? (See external threats section).

Are mechanical keys and locks appropriate to threats?

- Is each mechanical lock still an acceptable solution?
- Are restricted keyways needed / in use?
- Do deadlatch mechanisms work as intended?
- Are cylinders snap protected where appropriate?
- Are we using key safes or cabinets to store sets of keys? If so, are they suitable, secured behind multiple layers *and* concealed?
- Consider key management – are any keys held externally in key safes or by external companies and is this tested for robustness?
- When were keys last issued? How many have walked in that time?

Are card / access control technologies appropriate to threats?

- Is our system routinely reassessed in context of evolving card cloning threats? *The Flipper Zero and smartphone apps are changing this landscape quick, fast and in a hurry – it's like being able to copy a key when it's in someone's pocket.*
- Are the risks of the reader communications protocol understood? If we use Wiegand, clock and data or OSDP V1, do we understand the risk?
- Are reader, enclosure, etc tampers connected? Do they alert when triggered? Who is alerted, how urgently and what is the response?
- Do we know which locks fail secure or fail safe? Are battery backups in use? Are we satisfied with the design compromises?
- Are fire integrations balancing risk and security appropriately and are exit delays or other features worth considering? Has this balance of risks been reviewed recently? Do fire safety systems present security risks we need to consider?

Controls

Is RBAC / HR syncing in place?
- Is physical access restricted by roles?
- Is there a robust process for removing leaver and visitor permissions from PACS? Is this audited?

Additional features enabled / utilised?
- Anti-passpack, time limited access. *These features often just need configuring – you've paid for it, use it!*
- Do we need to consider integration of PACS, CCTV, alarms, etc?
- Is 2FA (e.g. PIN + card) considered where risk is increased?

Are keys, cards and people audited? Can they be?
- Do we know whereabouts for issued keys and cards?
- Do we review PACS access to ensure it's aligned with roles?
- Are cards reissued to new employees when returned by leavers? Is the cloning risk acknowledged and understood?
- Can we check where people are and have been if required?

Are controls installed securely?
- Is power and communications wiring protected? *Common issues include being loose in the ceiling void or connection boxes for conduit being easily accessed.*
- Are retrofitted electrified strikes sized to avoid introducing a latch slipping risk? *This is <u>really</u> common and is a balance of cost Vs security.*
- Can someone unscrew important things which are mean to be secure? *E.g. mag locks, connection boxes, door controller panels.*
- Consider whether exit buttons can be reached from outside or whether disabled access buttons bypass any authentication steps.
- "Security screws" are often used – consider whether this are overly relied upon for their real-world level of security.

Are servers for controls / DVRs within the cyber security remit?
These systems are often advertised as being a "physical security asset" and not needing to be under the remit of cyber security. Most door controllers are a Linux computer running an ancient kernel, the admin software often runs on outdated versions of Windows and all connect with Ethernet. This categorisation as "physical security assets" often inappropriately segregates them from cyber / infosec risk assessments.

Just like any other IT asset, consider: isolated VLANS/LANs, firewalls, can they reach the internet, patching, data held onboard cameras / sensors, PII etc.

PACS Credentials

PACS credentials refer to the tech in the RFID tag used to identify that card. They can be modern and using encryption or simply spit out a number.

Just because an old or cracked credential type is in use does not mean a system is inappropriately used or completely insecure. This being said, a vast number of companies are using credentials which are no more secure than a early 1990s system. These can be easily copied from a distance whilst someone is wearing or carrying a badge. There are many other PACS attack vectors including MITM attacks.

It's way beyond the scope of this document to go into the types of credentials which are vulnerable or what makes a secure system. It took me months to write that training course. So I've settled for the below…

The below represent red flags and further assessment:

125KHz – This refers to low frequency credentials which are almost always trivial to clone.
Paxton Net 2 – This system is ageing and likely uses HITAG2 cards in password mode. The password has been known for years and turnkey cloning tools are on Ebay. This isn't exclusively the case – it can be better or worse.
CSN – Meaning "card serial number". This means the system uses the CSN to authenticate the card. The CSN is exchanged in the initial handshake and isn't protected information. CSN mode likely ignores advanced encryption technologies and needs investigating further.
Mifare Classic – 1997 era tech with broken encryption, key and implementation issues. It can be implemented well but usually isn't. Flipper Zero can clone bad implementations (most of them).
iClass – Comes in many forms. iClass legacy is on par with Mifare Classic and from the same era. iClass SE however is somewhat better. There are standard and Elite keys to complicate things. Flipper can test using the PicoPass application.
Wiegand – A legacy reader to controller communications protocol from the 1970s still in widespread use. Sends data in the clear. MITM attack tools cost £30 and are trivial to fit.

Remember to judge each system against the threat model and in the unique setting where it is deployed.

Offices, Rooms & Facilities

Are office and facility use changes updated on registers?
- Is an inappropriate office being used to store boxes of old HDDs "*temporarily" (i.e. for the last year and likely for at least one more).*
- Have office assignments changed (formally or informally) leading to change in the material risk? *E.g. unmanaged office swapping.*
- Has the content of offices or stationary cupboards changed materially? *Are we storing confidential information (or that box of HDDs) in areas secured for only pens and paper?*
- When risk registers are updated, does this drive reassessment and remediation of the risk? Is this checked for efficacy? *A risk register without a plan is just a list of accepted problems.*
- Do we handle security requirements for risks to individuals and business differently and is there a reporting mechanism for both?

Is RBAC / auditing appropriate and facilitated with PACS?
- Is specific training needed to access equipment or areas, warranting physically restricted access? Are rights reviewed?
- Should access be audited? Can be it be audited?
- Is internal CCTV desirable and justifiable?

Have we considered counter surveillance?
- What can be seen from outside? Window films? Any adjacent public buildings which could make a good OP? *E.g. car parks.*
- Are projector connections secured or at least difficult to access?
- Is the room secured and access restricted?
- Are more advanced technologies like laser mics a risk?
- Is EM emission a concern?
- Are phones surrendered and how are they stored?
- Are there general meeting rooms and secure meeting rooms?
- Do we know what the inside of floor boxes, panels, card readers, etc are supposed to look like? *Would we notice extra devices?*

Counter surveillance thought exercise:
Would staff question a box plugged in the back of their PC marked "Property of IT, do not remove"?

If not, what can we do to make them ask questions? How can we generalise that curiosity outside of this example?

Offices, Rooms & Facilities

Looking up, have ceiling void risks been considered?
- Does the ceiling void allow access into higher security areas or between controlled zones?
- Is there unprotected wiring within the void? (Ethernet, PACS, alarms).
- Are conversations audible in adjacent rooms through vents or voids?
- Do drop ceilings make it easy to plant surveillance devices?

Looking down, have floor box risks been considered?
- What is in the floor boxes and is it a potential target?
- Is there a risk of accidentally bridging networks?
- Do they need securing / regularly checking?

Are there any risks associated with OT?
- Are these security or safety risks requiring extra security?
- Are these exposed data connections (USB, RJ45, serial, etc)?
- Are tamper evident seals in use and regularly inspected?
- Are controls protecting OT the same controls protecting building access? *It's not uncommon for OT to be protected by the building PACS tappy tap system. This is a major target and likely to be compromised by an even mildly technically capable adversary, therefore different or additional controls are required.*
- If crucial OT systems have open physical ports, should they be afforded similar security to a data centre or similarly vulnerable area?

How are secure rooms and facilities cleaned, secured, etc?
- Are external companies used?
- What vetting is performed? Is it appropriate? Is there any?
- How are sets of keys or lists of access codes held and used?
- Would anyone notice a strange addition to the cleaning team?
- Might these team members (with wide ranging access) be vulnerable to elicitation, financial manipulation or social engineering?
- Is this an approach threats to our organisation might use?

Are controls bypassed by stairs or lifts?
- Are lift security controls potentially bypassed? Are the control keys common keys or bespoke? How are they managed?
- Are there routes past controls by using stairs to go around controls? *These gaps can be found on fire maps displayed in buildings.*
- Are evacuation routes assessed for introduced vulnerabilities?

Monitoring

Do we need surveillance or security?

A common statement is “we have CCTV” usually with some confidence. The question is “...and what’s it *doing* to reduce our risk?”.

Surveillance – records and allows review of / reconstruction of events. Allows us to see what’s going on but is very passive.
Security – triggers actions based on detection capabilities.

E.g. – door access logs which stay on a controller are surveillance tools, whereas triggering action based on events is active security.
E.g. – CCTV cameras which record only are surveillance. Cameras which alert to a person within the server room provide security.

Ideally we want to see a plan built from a security risk assessment which shows a list of events requiring alert triggers (intrusion, water leaks, etc). The plan should map these out - what is a trigger for CCTV alerts? Who is alerted and how? What is the expected response and urgency? Then we need to see how this system and response is tested.

Integration

Most access control solutions allow the integration of cameras into PACS. The extent can be as simple as an alert triggers and it shows the operator the 5 seconds before the alert and the 5 seconds after from the camera monitoring. It can be far more advanced and the more expensive access control solutions advertise extensive integration with a huge range of building management, security and other systems.

The impact of integration can be synergistic but it can be expensive to configure and maintain. You might find the ROI is debatable. Most basic systems offer a degree of integration which may be achievable by internal estates teams. You might find you’re paying for features which allow a proactive security posture – such as alerting to improperly closed doors out of hours or counting people Vs card presentations.

Imagine a system which alerts through the alarm sensors, PACS indicating a door is open out of hours and through CCTV motion alerts – three systems with independent sensors all reporting an intrusion leading to a higher chance of a full police response Vs a simple alarm trigger.

Monitoring

Do sensor alerts illicit an appropriate response?

- Does a detection in the office bar (why can't I work in a place like this?!) send an email for CCTV review? *Remember that insider threats usually start small and normally follow a three-step escalation before a significant breach. Catch them early.*
- Does a detection in the server room trigger an alarm / lockdown?
- Are sensor / reader tampers connected and do they alert anyone?
- How do alerts requiring immediate interdiction work? On site security? Police? Cross-trained first responders? Lockdowns?

Is data from events used to drive continual improvement?

- Are we addressing false alarms and not just ignoring them, normalising deviance? How do we deal with alert fatigue?
- Are we addressing causes of repeat true positive alerts?
- Rather than just sighing at employees subverting security measures, are we taking data to senior leadership and advocating for training?

Are alarms, alerts, etc routinely tested?

- Is the testing schedule based on risk of harm or failure?
- Are responses routinely tested? Does everyone know what to do?

How is monitoring data transmitted?

- Wireless cameras are common but may be another "physical security" system which is out of the scope of the cyber security team. Is this data encrypted and treated the same as any other sensitive data?
- Are PoE CCTV systems secured in the same way as any other Ethernet connected device?

<u>How is surveillance data integrated into the ISMS?</u>

Aside from CCTV recording retention, consider that:

- Some alarm sensors will hold event data on the sensor itself. This could include video footage. Common on sophisticated, stand alone sensors (e.g. LiDAR) which have simple integration with an alarm.

- Door controllers will hold access permissions and logs on the controller. What is held and is this personally identifiable?

- If biometrics are in use, what data is held on the device, how is it secured and is this device in a low security area? Most devices since 2011 are fine, but likely contain special category data under GDPR.

External / Environmental Threats

Are environmental threats understood and controlled?
- Floods, locally stored / used hazardous / explosive chemicals, gases.
- Do we have plans if the above hazards do manifest?
- Do we review these plans if threats change? *E.g. introduction of a new flood management system that ironically means we need to put the servers higher up as we're in a newly designated flooding zone.*
- Risk from local industrial accidents or automotive accidents. *Does there need to be a plan for when staff are unable to attend office?*

Are suitable emergency drills held?
- Beyond fire and evac, do we need to consider lockdown drills?
- Do we have special hazards requiring drills? Are there evolutions?
- Have we tested our incident detection and response? *This includes involving the "shop floor" team, not just execs at a strategic level.*
- Do we take the results of tests and alarms (false or not) and use them to drive continual improvement?
- Is there a debrief after false or true alarms to address the cause and any action to take? Is this recorded and reviewed?
- Do we review fire prevention, containment and evacuation strategy after false alarms and incidents, using them to drive improvement?

Are car park related hazards adequately controlled?
- How possible is it to attain unsafe speeds within the car park? *Car parks with long runs could see accidents at higher speeds. Twisty ones may increase the chance of pedestrian collision. Note that small increases in speed present disproportionately higher hazards.*
- What threats are posed to staff walking to / from cars? Is this a public, private, secure or highly secure space? Are protections adequate?
- Is there a sufficient stand off distance between parked vehicles and buildings with respect to fire?
- Has fire risk with respect to EVs, hybrids, etc been re-evaluated and is this assessed regularly giving the evolving knowledge and experience?
- Are e-bikes, etc stored / charged on site? Is this risk considered?

Fires caused directly by EVs appears to be a low probability event, but those involving EVs / hybrids burn at higher temperatures and produce high volumes of extremely toxic and explosive gas. E-scooters and e-bikes appear to be a more significant risk, often brought inside and / or charged. Are these different risks considered and controlled for?

External / Environmental Threats

Is the external lighting suitable?
- Are all pathways, entrances and car parks properly lit?
- Is lighting sufficient to see faces and numberplates?
- Might any poorly lit areas aid in entry or hostile surveillance?
- Do staff feel safe with current lighting arrangements? *This is a big one. Part of my assessment process is to turn up the day before and ask local, evening businesses how safe their staff feel coming and going. On-site lighting plays a huge part in this, impacting stress / morale.*
- Is lighting sufficient all year round, are timings adjusted seasonally?
- Are high voltage connections to lighting systems properly protected?

External Infrastructure Dependency (Mostly CNI):
- Are mitigations in place for a power failure and do we know how security systems behave? Is there a risk of information loss?
- Are we prepared for a BT copper infrastructure switchover? Have we accounted for the new risks?
- Do we need and have a no-comms plan? Should this include internal and external comms? Is it usable with little familiarity?
- Are local transport links prone to flooding or other kinds of failure? What is the impact? Does WFH capability impact the preferred plan?
- Are we reliant on fuel and do we keep a reserve?
- What infrastructure problems could affect critical suppliers?

Vandalism, political, religious violence – do we keep updated?
- Have we mitigated the impact of vandalism to an inconvenience?
- Do our business activities or personnel expose us to backlash from political, religious or geopolitical events? Have we controlled for this?
- Are increased risks from the above communicated to stakeholders?
- Are staff personal safety concerns heard and addressed? Is there a formal process to report and resolve (or justify why no action taken)?

Surveillance, EM spectrum:
- Is visibility into the building controlled?
- Are longer range WiFi / RF attacks considered? (Consider LoRA based industrial controls, disability door openers, remote shutters, etc).
- Are drones a threat (surveillance, RF, WiFi attacks) and how is this mitigated? Can it be mitigated? If we can detect, can we interdict?
- Are we keeping an eye on drone / counter drone technology, emerging trends and defences?

Secure Areas

Keep in mind the threat.
- Who is targeting what and how?
- The secure area has a full perimeter.
- The secure area is relative and impacted by the changing threat, risk, business operations, adjacent controls, etc. These all affect each other.
- Ensure the threat is defined before any discussion about a secure area takes place. More detail in Equipment Siting / Protection.

Have we re-assessed the need for a secure area?
- Secure areas might be a hangover from when data was held in paper form. The risks the secure area was managing may no longer exist or may require different controls. There is an ongoing cost to maintaining secure areas and this budget can be redirected to better cyber security controls if appropriate.

Audits are a good time to reassess:
- Can and should multiple secure areas be consolidated? (This may have implications for insider threat).
- Have activities requiring secured areas expanded outside of designated high security areas? Why? How to resolve? *Migration from paper and remote working have facilitated this. It is absolutely within the scope of the criminal to target a work from home environment, people on trains or simply working on a laptop in the staff cafeteria – a "private" but not "secure" area.*

Are additional access controls present and appropriate?
- Are controls layered in addition to building access controls? *E.g. separate SIO held on access card with different encryption key, PIN, intercom.*
- Limited to those who need access (RBAC using PACS).
- Is some kind of 2FA needed? (e.g. card and PIN).
- Are internal entry / egress cameras justified and do they capture faces, not just bald spots? Could someone familiar with the area evade these cameras?
- Do declined cards generate alerts to be reviewed (+/- CCTV)?
- Are permissions routinely audited?
- Have changes in fire regulations or other compliance requirements been assessed for security impact?
- Is human camera verification needed for access? Is the process tested and is it known that it is tested? *Normalised deviance is very much a concern with these systems – do people just press "open"?*

Secure Areas

Are insider threats controlled?
- Is activity monitored? Can it be? Should it be? Must it be?
- Is collection of activity data from within the secure area passive logging or an active security measure? *Lookin' at you, GCHQ…*
- Are cyber-physical controls like port blockers, floor box locks used? Can people physically connect external devices like phones, portable media, etc? *So, uh, GCHQ, we should talk...*
- Is there egress filtering / screening? Should there be? *GCH… Oh never mind, they clearly know better.*
- Is there a SIEM system flagging out of pattern area access or computer use? Are potential intrusions mapped, triggers and thresholds defined, and then acted upon? *GC… Okay, that horse is dead.*
- Are there hidden processes which are not known / visible to staff? *This includes monitoring with a high threshold for triggering action and concealed hardware (e.g. secondary or silent alarms).*
- Are staff aware that everything they do on company equipment is monitored? Are they aware of the extent of the monitoring?
- Have we taken specialist advice on privacy law for our monitoring?

Is the working environment comfortable and temperature sensible?
- Everyone knows the audit is happening. If the room is baking hot and everyone is sweating, look for evidence doors are routinely propped open when you're not there. *A/C can be a security investment!*

Are we granting persistent access without necessity?
- Is granted access to high security areas persistent? Or is it only granted temporarily on request and monitored?
- Do employees with a different home-site or without regular access needs have to request access when required?

Have we revisited external threats with respect to the increased risk associated with the secure area activities?
- What can be seen from outside? Are laser mics or advanced kit a concern?
- Any RF / EM leakage to consider? (See the counter surveillance section in Office, Rooms and Facilities.)

The "secure area" essentially revisits the perimeter, controls, monitoring, etc. It is essential that we at least require different skills and tactics to overcome secure area controls compared to the general building security.

Equipment Siting / Protection

Before considering if equipment is properly secured, establish:
- The business value (inc. opportunity cost and replacement lead-times), replacement value and criminal value.
- Any risk associated with unauthorised access (data loss, injury, etc).
- What data is held on the device and is it routinely removed?
- The visible exposure – is it on display? Are there barriers?
- Has the risk materially changed since the equipment was sited? *It's possible external security has actually improved, reducing the risk or the equipment may be out of production and more valuable for parts.*
- Assuming we have considered protecting the equipment, have we considered protecting people – safety risks, curious teens, etc.
- Do we have a risk register entry and contingency plans for mission critical equipment without which the business can simply not operate?

Consider the type of physical risk:
- Opportunistic: The impact from opportunistic criminals / vandals should always be "inconvenience" or less wherever possible.
- Targeted: This is, by definition, organised crime to a greater or lesser degree. It usually involves a team, hostile surveillance and determination. The most effective way to deal with this is to make it obviously impractical at the planning phase.
- Insider: Equipment protection against insider threat is tricky as these people have functionally infinite time to observe and plan at close quarters. Insider threat usually manifests with small, low key pokes at security before anything large. Detecting and acting on these is key. It may be that some security measures are not revealed to staff – see the Secure Areas section for more on insider threat.
- Cyber-physical: Where the two worlds meet, gaps appear. Unauthorised access to equipment may allow cyber attacks by introducing USB sticks to networked, but vulnerable equipment. Or physical damage / security impairment could be caused by cyber attacks. PACS card cloning could be considered cyber-physical as could deauthing / hacking cameras to create blind spots.
- Sabotage: This may be isolated or part of a shaping operation for a larger attack. It may also fall under all of the above. Sabotage may be motivated by competition, ideology, ressentiment / resentment or simply represent opportunistic vandalism.

Remember the risk of drones. Small, cheap drones can be used to get malicious electronic devices within close range or to cause physical damage to equipment previously thought inaccessible.

Equipment Siting / Protection

- Is there a business continuity plan in place? *And has this been developed with the people on the ground who have to implement it? For mission critical kit, there should be multiple contingency options.*

- Is there justifiable value to displaying equipment? *Equipment on public display makes hostile surveillance much easier. The best time to deter an attack is to make it appear unfeasible during the planning phase. Displayed equipment can make us a self-selecting target. Consider ram raids and other "brute force" attacks in such settings.*

- Are we relying on equipment being secured to the ground / workbenches? *Especially when equipment is being stolen to break for parts, irreparable damage may be caused during removal attempts. Even if the theft fails, the equipment may still be lost.*

- Are supporting systems protected? *Servers are the classic example where dependence on HVAC, power supplies and telecoms means a huge amount of supporting infrastructure needs protection.*

- If we are to add layers of security, do they introduce new skills to overcome them and additional detection opportunities? *It's easy to say "we'll just put another fence up around the vehicle yard" but if that fence can be breached using the same tools as the existing outer fence, and there's no additional intrusion detection prior to the vehicle alarm, you may not add much in the way of effective security.*

- Can we add any pro-active security? *This could be as simple as detecting doors aren't properly closed at night, or highlighting nocturnal vehicle activity in an area usually dormant. FLIR sensors can be used to detect people, and also equipment / environmental temperature changes. How might sensors or monitoring kit might be used? Ask whether PACS access is audited and if any access codes are routinely changed (e.g. digilocks). What about social engineering mini pen tests?*

- Can we add better reactive security? *People ignore alarms and criminals know. But a siren and a voice through a PA system might make someone think that this is no automated system. AI systems taking a description of the person from CCTV to personalise the automated message are coming soon to a dystopia near you… Smoke and blasters make it difficult to operate effectively whilst breaking down communication, and may cause teams to leave before being caught.*

Main Entry / Reception

What impression does the company wish to convey?
- Welcoming or high security? What are the implications of the choice?

Are we considering this to be a strict control or do we consider the building porous, where people can easily move in and out?
- Where access is shared with other businesses, the building immediately needs to be considered porous as we have no control or assurances regarding access card security or other company policies.
- A porous building may not require constant main reception monitoring as there's little benefit for the resource.
- A strict building perimeter and main entry control will require significant additional resource, not just at the main entrance, but all others.
- An attacker facing a porous perimeter may face less challenge when entering the main building but more risk when entering the office space of the client. Faces are known and there's not a perception of a secure perimeter.
- An attacker facing a strict perimeter will often find a sense of security and assumed belonging when within the building.
- Whether these controls are strict or porous massively impacts how security is handled, and where / how the risks need to be controlled.
- Consider, from the attacker's perspective, how you approach porous / strict targets differently and where you expect controls to be.

How is the space classified?
- Public? Private? Secure? Transitional? Is the classification appropriate?
- What risks does this create and how are they controlled?
- *As an attacker, consider how you'd use / abuse transitional spaces.*

Is there an admission mechanism into the reception?
- Intercom? PACS? Camera? Open door?
- What risks does this create? *Intercoms are a perfect place for normalised deviance to creep in – verification is an inconvenience.*
- Is the actual level of protection provided understood and suitable? *It is worth asking if a well positioned door-closure blocking pen, tailgater or other low-tech attack can bypass a high tech access control system.*
- Do other companies / people share access or admission capability? If so, is this effectively public access for the purpose of our security?
- Finally, are we using external key boxes for out of hours or contractor access? If so, why? Are there alternatives to this security nightmare?

Main Entry / Reception

Is the reception area manned?
- Is the area manned at all times?
- If so, is there a process to relieve for human needs or shifts?
- Do other operations, such as customer relations, deliveries, etc rely on continual manning? Do we separate security / reception functions? Why?

Is social engineering considered?
- Are loiterers noticed and challenged?
- Is information regarding loitering, visitors, etc handed over between shifts?
- Is there a robust visitor process? *See Personnel Screening and Security Awareness sections.*
- Are unexpected visitors routinely challenged and is this mechanism tested?
- Are employees from other sites classed as visitors, requiring advising reception in advance?
- Are there policies which protect the business interests against humanitarian actions? *It is absolutely not beyond me to get out my crutches and a box of books, a fake ID for the business (which doesn't open any doors) and get someone to let me in. Or to show a "Just Can't Wait" card and pretend I've got IBS and I reaaaaallly need to use your toilet. Policies and controls should allow staff to be human, help others in need whilst protecting the business against anyone trying to exploit this.*

Are building plans on display?
- Must they be on display? Can they be locked in a "fire" box?
- Do these plans have to display the location of sensitive areas like server rooms, or can this be renamed "electrical room" reflecting hazards but not advertising location of vital areas?
- Even a sanitised plan, on display, is gold for an attacker. It allows them to plan where they're going and ensure they never look lost.

Are controls tested?
- Are senior execs turning up at site and trying to bypass the visitor policy? Are people challenging them rewarded?
- Are simulated breaches (e.g. social engineering, testing visitor policy) routine? *These can be performed at relatively low expense and ensure staff have the real world experience challenging people as well as avoiding normalised deviance which is easily recognised and exploited.*

Delivery and Loading

Is the loading area subject to the same scrutiny as the main entry?
- These are usually classed as “private, insecure transitional spaces” which makes them tempting targets. Do we protect the area in line with this or is it often left to chance?
- Do we ensure surveillance / manning is as strong, if not stronger than the main entry? L*oading areas often have valuable information, stock or hardware and present safety hazards.*
- How are human factors controlled? Are there processes, controls or architectural features? *It’s very common to find doors propped open, people taking breaks or otherwise leaving the area unmanned and insecure. Ask what the likelihood of this happening is and what risks it poses to the business.*
- Is the loading area a known shortcut for staff or a regular smoking area? *This isn’t necessarily an issue as long as the risks associated with this use are controlled – it will happen, so deciding where is key.*

How does the loading area integrate with our perimeters?
- It’s not unusual for a loading area to provide a complete, insecure route through all perimeters. This is obviously not ideal and I suggest walking this route to see if you can gain entry.
- It is not usually difficult or expensive to harden this route, but it usually requires routine, internal auditing to ensure procedural compliance.

Is equipment, stock and data protected?
- Are computers hardened as per the area classification? (e.g. “private, insecure, transitional”).
- If CCTV is relied upon, is it active security or just surveillance?
- Is mission critical equipment or expensive stock stored here? Does this change how security is seen? See Equipment Siting / Protection.

Some adversarial questions:
- Would hostile surveillance be detected? It’s often a good opportunity to detect people snooping around as we rely on being ignored.
- Does parking / stacking create camera or observational blind spots which aid adversarial movement by providing concealment?
- Do seasonal changes in sun position cause camera lens flare or contrast problems which could be exploited (by external or insider)?
- If someone tried to walk in with confidence, do we have confidence they would be challenged?

Mobile Assets

Who would want to take them and why? Is there risk of loss or damage?

- What is the threat and what impact could they have?
- What kinds of mobile assets do we have? Sometimes this is vehicles, often it's laptops and smartphones.
- How might someone use mobile assets to damage the business?
- How might human factors create risk via mobile assets?
- How do we ensure the loss of a laptop results *only* in the loss of a laptop, and no data or access is put at risk?

Are we relying on tracking systems?

- Criminals now mitigate for trackers routinely – them leaving a vehicle to "cool off" can present an ideal recovery opportunity. Do we have a plan to exploit this?
- Consider a decoy tracker hidden in the more traditional places, which can help keep the real one in situ.
- Smaller items like laptops or phones can be placed in Faraday cage style bags to block trackers until they can be dealt with.

Have we considered the risk of work from home?

- Whilst people's homes are generally considered off limits for security assessment and testing, criminals don't have the same limitations.
- Some internet fraudsters are now placing surveillance devices within victim's homes to try and intercept 2FA tokens.
- If we have high level people in the business working from home, consider the risk of technical surveillance measures if there is a risk from industrial espionage, etc.
- Do we need a basic level of home network security or is this risk mitigated by our VPN, etc?

Do we have a policy about public work?

- Providing a laptop for working from home creates a lot of flexibility but increases the chance of people working in insecure environments.
- There is a risk of people overhearing conversations or seeing documents in public spaces.
- Have we balanced the increased productivity against the risk? Are we happy with employees routinely working on the commute to work?
- What information could someone get about our information security measures by viewing the Windows desktop? Can we mitigate this?
- Do we issue laptop cables, privacy films and use features to automatically lock laptops left unattended?

Mobile Assets

Do Mobile Assets (e.g. laptops) Increase Insider Risk?

- Other risks may include exfiltration of data by insider threats. Even if a system is well protected against data exfiltration, there's nothing to stop someone simply taking videos of screens, recording conversations, etc if they work from home.
- Could smartphones be cloned or SIMs duplicated with the employee's cooperation?
- If a leaver fails to return a laptop, can they access any data? Is there a way to disable that laptop whilst we still have access?
- Are employees fully aware of the level of monitoring and logging which occurs on work laptops and smartphones? This is covered in more detail in secure areas and can help discourage insider risk before threats actually manifest.

Do we provide training and awareness around the unique risks that mobile assets present?

- Are employees aware of the risks of public work?
- Do employees protect their work laptops and assets as their own?
- If a compromised device was sent "from IT" to an employee's home address, would they connect it to their laptop if instructed?

The loss of vehicles (temporary or total) or theft from them is almost a certainty over enough time – how are we mitigating the risk?

- Are any vehicles critical business assets?
- Is there a plan for replacement or rental?
- Do we have effective systems to ensure vehicles aren't left unlocked?
- How do we prevent the loss of data from vehicles? Is printed customer information or similar left in the vehicles?
- Do we store keys to protect against relay attacks?
- Are there any risks of data theft from vehicle data systems / sat navs and are these risks significant?

Finally, asking the obvious, is there an up to date register of assets, who has them and where they are?

- Is this routinely checked?
- If the asset disappears, are alerts raised quickly enough to prevent further issues?
- Who does what, when and how when business critical or information rich assets are lost?

Personnel Screening

How is insider risk assessed?

- Do we have politically or ethically contentious operations or supply chain / services from companies with such operations?
- Is this risk liable to change and is it reassessed with current events?
- Are we monitoring using data loss prevention systems to detect and alert to unusual activity? If not, should we?
- What level of screening is appropriate for potential employees?
- Is there a need to re-screen existing employees?
- Is there a system for flagging disgruntled employees?
- Are effective (not perfunctory) stress detection and management systems in place?

Is there a *specific need* to make use of the following?

- DBS checks / update service (note basic, standard and enhanced).
- Personal social media screening.
- Credit checks.
- Review of activity / logs (as described in secure areas) be reviewed for concerning activities before internal promotion to sensitive positions.

Note that, aside from specific situations, significant justification is required for much of the above. There's a real ethical / legal risk inherent in performing these checks. Legal specialist review is mandatory, along with strict adherence to approved procedure by staff.

Are visitors managed appropriately?

- What approval is needed? Is vetting required? Is there a pre-approved list? *Schools may require a level of seniority to authorise external visitors and then DBS checks on the named individuals to visit site, only allowing those people on site after formal identification, for example.*
- Is an escort required? *This can be for the visitor's protection as well as the business, depending on the setting. This is resource heavy if done properly and has high risk for deviation from policy unless policed.*
- Are visitors given PACS cards and, if so, is access restricted to minimal for each individual visitor? *General visitor's cards are often used with access to most areas.*
- Are visitor cards disabled on PACS admin software when returned? *If a visitor's card is cloned then, by deactivating it when out of use, the clone can not be used until that visitor's card is reissued.*
- *Are visitors identifiable as such by employees? Visitor's badges are seen as old school but allow our employees to detect intrusion.*

Continues over...

Personnel Screening

From previous page...

- Is there a process for validating visitors without approaching?
- Are devices held at reception or outside secure areas? *It's easy to say "we aren't searching, what's the point?" but, the lack of phones has other advantages and surveillance can't be concealed in plain sight.*

Thought exercise: How might threat actors use our visitor, recruitment, delivery or induction processes against us?

Starting points:
What information is in job adverts.
Replica visitor badges or passes (physical and RFID clones).
Social engineering reception, abusing processes, "it's my first day!"
Abusing delivery processes; theft, infiltration, vandalism.
Now, where are the opportunities for controls or mitigation?

Identifying struggling departments and employees quickly and resolving problems is very much a security adjacent function.

Deciding on intervention requires discriminating between the following:

Resentment is short-lived bitter indignation when we perceive we've been wronged. It typically manifests as temporary ill will toward the identified cause and resolves through self-reflection and dialogue. Over time, we acknowledge our own part, commit to self improvement, and establish boundaries. For example, if we don't secure a job we believed we deserved, we might resolve to addressing identified skills gaps and quietly decide "I just won't help them out in that area until they see my value." Resentment is usually self-limiting and best left to resolve.

Ressentiment describes a deeper, chronic grievance. It may be rational or irrational but is often characterised by simmering bitterness, and a sense of powerlessness against the causes of resentment. Rather than leading to introspection, it culminates in a vengeful drive to "even the score." The emotionally exhausted employee, feeling perpetually wronged, presents a high risk for insider threat and is a flight risk. Ressentiment almost always demands action for multiple reasons – protection of the business and employee welfare / duty of care. These individuals are usually in a chronic, cortisol mediated state of stress and prone to making poor personal and professional decisions.

Security Awareness

Penetration tests often use social engineering to enter a building. The question we should ask is “what risk are we emulating here?” Why might someone want to enter the building? What is the risk? Where does it come from? How does it manifest?

What risks to the business might require physical entry?
- Consider what they might be for this particular business:
- Journalists, information thieves, hardware theft, secret sauce enthusiasts, activists, domestic disputers, former employees, etc.
- This list forms the basis of a physical security awareness requirement. The sophistication and capability of the threat helps understand the risk.

Does the team have an acceptable level of security awareness? Ask these qualitative questions:
- Would they detect a stranger wandering the office, inspecting computers? How would they react?
- What about the stranger removing computers, equipment, data, stock?
- Do policies control for normal human vulnerabilities exploited by social engineers?
- Would anyone be able to blag or sneak past reception / loading bay?
- If an IT manager brings in their new partner, who doesn’t work there and doesn’t have clearance, and takes them into the server room whilst they do maintenance, would it be challenged? Could we test this?

Culture and processes:
- Is there a culture of / mechanism for reporting problems? Is this culture felt at a ground level or just leadership?
- If you ask “what would happen if someone reported a dodgy link they clicked?”, would the respondent be worried about reprisal?
- Are alerts triggered by clear attempted infractions (e.g. attempts to access secure areas or copy data) sent to managers to address?
- If issues (such as door propping due to heat) are identified, does management address with solutions, not enforcement?
- Is there a method of stopping and identifying tailgaters?
- Is there obvious management buy-in and adherence to the processes?

Have you thought about how we can demonstrate management buy-in to a security culture? Overtly testing using the IT manager scenario above and rewarding anyone who challenges, or more subtle things like senior leaders “forgetting” an ID badge and wearing a visitor’s badge per policy.

Security Awareness

Are drills, simulations or incident response testing used?

- And are they at least applicable if not realistic?
- Do they include everyone who might be involved in an event?
- Is this just a leadership exercise and, if so, why?
- Is it impactful beyond those immediately involved?
- Does it create a positive “can do” approach to incidents?
- Is there post-event analysis and feedback from all levels? Does this demonstrate the value of the feedback and does it make its way into policy changes? Are these changes credited?

Crediting policy changes to individuals, especially those lower down the hierarchy, is powerful. It avoids any accusations of “boss took credit for my idea!” but also instils pride and shows ideas are valued no matter where they come from, driving continual improvement.

Is security awareness education repeated beyond just elearning?

- Does it need to be? *Some industries deal with security threats routinely and may not have need for repeated training.*
- Do we make use of “mental reps” as a training tool. “What would you do in this situation?” Real world examples are very useful.

Ideally, we want security awareness training to instil a set of routines and principles that generalise outside of the training scenario. So a phishing email training should not just teach “don’t open the link!” This is the end action we want to avoid. It should instil a curiosity about the sender, legitimacy and risk of opening the email. This set of principles generalises to someone walking through the office with a USB stick and an affinity for exposed ports – consider the person, are they legitimate and what’s the risk of what’s happening?

Do individual departments have a nominated security person?

- I hate “security champion” as a name but this is a person who has, as part of their job, updates from the various security functions (physical, cyber, electronic) and ensures they are distributed and actioned.
- This allows for a more effective cycle of continuous improvement, gives an accessible point of contact for concerns and ensures updates to processes / policy are actioned… not left in the bottom of an inbox to cry tears of abandoned loneliness...

Disposal / Recycling

For data storage devices:
- Is there a mechanism for remotely deleting data when at risk?
- Are portable storage media stored, destroyed or sent for disposal?
- Can we track the location / state / fate of all storage devices?
- Is evidence required and kept for disposal of storage devices?
- Is there a system that flags if a device has been removed from service but is awaiting disposal after X months? What happens?
- If I were to remove an old HDD from any part of the system, would I find useful data and how long until it would be detected?

For paper:
- Are there cross shredders to use at the point of disposal or is confidential waste bagged and sent for destruction?
- If the latter, are these bags protected in the same way as plain text, confidential electronic data?
- Do we stop confidential data being printed where possible? Does this system work in practice? If not, why?

Maintenance

What procedures are in place to protect data / equipment during maintenance?
- Are these audited and tested? Should they be?
- Are contractors simply ignored or checked and supervised?
- Would an unexpected contractor be challenged or left to it?

Are critical systems maintained in line with manufacturer's recommendations?
- If not, are contracts and insurance immune from repercussions?

Cables

Is the following considered?
Are power cables protected from intentional or accidental damage?
Are communications cables protected from damage or intercept?
Are alarms cables properly protected and tamper evident?
Is there protection for PACS power and comms wiring?
Are network trunks boxed in or in secure areas (not exposed in toilets or cleaning cupboards!)

Distribution

This document is the product of many years of experience. I have spent countless hours distilling it down into key questions and tasks for you to consider.

Phil Smith – Styx Security Ltd.

Version

Version 1.1

Upcoming updates: Video guides linking to each page.

History:
Version 1.1 – Minor updates, link to videos webpage.
Version 1.0 – First major version, limited release for review.
Version 0.x – Limited distribution. ODS format.