

1. General - Understand the DIFFERENT terms & roles played (LSRA, SSP, yourself, and your contractors)<sup>1</sup>:
  - a. Reporting - Suspicious activity to Watchcon: 021 790 9333 (Voice) or 060 345 3514 (WhatsApp Text Only)
  - b. Response – Catching criminals in-the-act is most-effective for prosecution; but requires quick Alerts & Notification<sup>2</sup>
  - c. Public Space – additional security is provided by the LSRA, and charged on your rates bill; HOWEVER,
  - d. Roads & Trails – are open to the public 24/7 and cannot be restricted; so, you must still protect your property
  - e. Prevention – is otherwise best achieved by Owner maintaining effective Home Security Systems & Practices<sup>3</sup>
2. Home Security Systems & Practices - Basic steps cost little, and expensive BUT ineffective systems cause complacency<sup>4</sup>:
  - a. **Contractors – Give them this memo; insist on: user-friendly systems, training, and minimal nuisance alarms<sup>5</sup>;**
  - b. Maintained – Means fixing, but also properly setting-up and routine testing (see for each system below)
  - c. Testing – Final testing after initial install, and routinely, should always be done by Owner physically themselves
  - d. Temptation Removal & Precautions – easiest / cheapest solutions, for example:
    - 1) Strangers - Minimized; use known contractors; avoid subcontractors or temporary workers
    - 2) Conceal – Small / Valuable Property (cell phones, laptops, jewelry); keep curtains closed at night
    - 3) Secure - Weapons & Tools to avoid opportunistic use by criminals
  - e. Construction Sites – insist Owner’s take responsibility for their contractors, document workers, secure the sites
  - f. Unoccupied Houses – Owners/Agents must keep property secure with SSP contract to avoid squatters; remove mail
  - g. **Dusk / Sunset – Lock perimeter; set alarms / sensors / analytics from 6pm to 6am; but set perimeter for 24/7**
  - h. Access – Do not open doors for unknown persons or fake officials; tell your staff same; call SSP to if you are not sure
3. Physical Barriers & Miscellaneous – Routinely check for integrity/function and tampering:
  - a. Fence / Walls – Need especially next to public roads & trails; avoid bendable palisades; add foundation & spikes
  - b. Electric Fence – Flashing “On” indication light for verification; triggering home alarm; test with insulated screwdriver
  - c. Electric Fence Remote – Phone App to enable turning on/off remotely to avoid reluctance to use while away
  - d. Doors – Locked even during day; occasionally change keys & key-pad codes, giving separate code for staff<sup>6</sup>
  - e. Sliding Glass Doors – ensure they cannot be lifted off slides; don’t leave keys inside locks behind glass easily broken
  - f. Windows – Locked even during day; curtains at night; prevent “popping-out” by insisting glass is glued in frames<sup>7</sup>
  - g. Shrubs / Bushes – ensure cut-back away from under windows or places where criminals can hide their work
  - h. Signs – Alerts criminals that you have an SSP, and optionally an Off-Site Monitor remotely recording / alerting
  - i. Dogs – should be brought inside after dark to avoid the temptation for criminals to want to use poison<sup>8</sup>
  - j. Exterior /Perimeter Lighting – ideally on a common switch and/or tied to alarm / motion-detection system
  - k. Motor Vehicles Street Parked – Keep locked and without exposed valuables or exterior luggage, avoid hidden keys<sup>9</sup>
4. Alarm & Sensors – Demand custom adjustment to your system so that it is not a nuisance and user-friendly:
  - a. Phone App – To enable turning on/off remotely to avoid reluctance to use while away for fear of disturbance
  - b. By-Pass - Know how to By-Pass specific sensors that are over-active, until adjustments can be made
  - c. Siren, Flashing Light, Alert – Should activate inside and outside; alerting zone name triggered to SSP<sup>10</sup>
  - d. Panic Button – Located in quick reach, possibly in multiple locations and/or on key remote
  - e. Beams – Require vegetation trimming and some can be crawled under
  - f. Motion Sensors – Exterior can be oversensitive in the wind, and interior may be too late for prevention
  - g. Stay or Away Options – Should both be used, so intruders do not enter & wait for you to open safes etc...
  - h. Code & Safe-Word – Ensure all residents & tenants know so that it is used routinely
5. Cameras – Best protection combined with Analytics & Phone Notifications (see below), IF properly maintained & tested<sup>11</sup>:
  - a. Commercially – Installers provide competitive pricing that might omit costly but needed technological features
  - b. Ask Neighbors – For product/service reviews (LSRA uses HikVision ColorVu/Hybrid 2.8mm for short views)
  - c. Battery & Wireless System – Are quicker/cheaper installs, but require additional maintenance discipline
  - d. Settings – Do not trigger on motion only; use line-crossing/intrusion fine-tuned for sensitivity, duration, & min/max
  - e. Features – Motion activated LED light, color images at night, remote speaker, SD Card for onboard event recording<sup>12</sup>
  - f. NVR – Continuous high-quality record; but just Playback is often too late, rarely does it lead to catching a criminal<sup>13</sup>
  - g. **Internet Connection – So that Notifications are LIVE on a Phone App or remotely accessed for Playback to aid a chase**
  - h. Linking into LSRA System – Is technologically challenging & costly, easier is to relay private alerts to OmniVision<sup>14</sup>
6. Camera Analytics & Notifications – type of “A.I.” that uses motion detection with filters to alert, then sends notification<sup>15</sup>:
  - a. Firmware (software IN the camera) - New generation cameras have built-in free software sufficient for home systems<sup>16</sup>
  - b. Set-Up – Camera Installer should make basic set-up; then train Owner in fine-tuning, or recommend a Specialist<sup>17</sup>
  - c. Interconnection – Specialist for: Camera to NVR to Router/ISP to Phone/Off-Site Monitor to Owner/Responder<sup>18</sup>
  - d. Testing – Via Owner’s live tripping: during initial set-up, again after 1-week, and then again every 3-months<sup>19</sup>

- e. Specialist – If Owner needs help, Camera Installer can recommend a Consultant Service or Off-Site Monitor<sup>20</sup>
- f. Off-Site Monitoring – Company can provide remote service contract to Owner, after camera install, as follows:
  - 1) Recording camera alerts as a back-up to the NVR, preventing the need for criminals to find & destroy NVR
  - 2) Monitoring camera alerts by a human operator for additional filtering of suspicious activity before alarming
  - 3) Notification of Owner and/or Responders as desired; and follow-up/play-back during/after an incident
  - 4) Sharing Incident Notifications with Omnivision (LSRA's Off-Site Monitor) to relay to PPA, Watchcon, SAPS, etc.
  - 5) **Specialist service to remotely set-up / interconnect cameras & test (even without a Monitoring contract)**<sup>21</sup>
- 7. Home Alarm Response - Private "Security Service Providers" ("SSP") provide contracted Armed Response to Home Alarms:
  - a. Private Property – Responder can only enter if: invited on site by resident, Category 1 crime in progress, or contracted
  - b. Limited - To normally only ringing your doorbell when an alarm is sent to their control center
  - c. Quality Company – Private choice, but recommended to select a company that participates in Community Security
  - d. Sharing - Incidents with WATCHCON to enable Public Space chase assistance must be in the contract with the Owner
  - e. Lock Boxes with Key/Remote or Shared Codes - With SSP allows them to check your property in case of an alarm<sup>22</sup>

END-NOTES – For additional information and background on above:

<sup>1</sup> SSP (Security Service Provider) in the area include: ADT, DeepBlue, and PPA (the latter is also the contractor for the Public Space response by the LSRA)

<sup>2</sup> SAPS Case numbers must be filed by the victim, otherwise no follow-up can be done by SAPS etc...; call WATCHCON for advice.

<sup>3</sup> Liability for Crime-Fighting performance is with the Owner and cannot be taken-on by any contractor. Unfortunately, there are just too many links in the system to put responsibility onto any one contractor. Hence why self-testing is so critical.

<sup>4</sup> Expensive systems can lead to a false sense of security; especially when they are so complicated, they are not used. The Owner must be involved in the design & selection of the system; there is no one answer or industry standard. Ask neighbors for advice on what has worked.

<sup>5</sup> New Technology makes everyone feel intimidated, and contractors often do not quote for excessive amounts of time to spend on training and/or troubleshooting to attain each Owner's specific preferences that evolve during the installation. Be prepared to pay more for extra training and follow-ups, until the system works without generating excessive nuisance alarms (over-sensitivity can make the system useless).

<sup>6</sup> Keypad systems often have a memory of WHICH code was used, so if a criminal gets access to the code, it will narrow down how they got it.

<sup>7</sup> Window installers unfortunately prefer to leave glass loose in the frames for easy change-out in-case of damage during install; however, this leaves the window glass very easy to remove with a simple technique; therefore, glueing to the frame is essential.

<sup>8</sup> Criminals will often "case" (inspect in advance) locations to rob by patrolling / testing during the hours they intend to steal; thankfully it has never happened here, but reported in other areas.

<sup>9</sup> Thieves have targeted recreational vehicles (exterior fuel tanks, bike racks, etc.); as well as looking for hidden keys left by surfers.

<sup>10</sup> New alarm systems will tell the SSP (and yourself) which sensor triggered (for example "Back Fence")

<sup>11</sup> **Camera analytics can send a screen-shot direct to your phone of an intrusion, which enables you to immediately SEE if it is a real problem or not. Beams & Motion detection alerts are often ignored because they cannot be immediately verified...so Owner assumes it is a false alarm.**

<sup>12</sup> SD Card on some make/models also allow for more efficient review of nuisance alarms to enable adjustments (this is a critical feature in the LSRA's ability to maintain the effectiveness of the Community system).

<sup>13</sup> SAPS has rarely been able to catch a criminal based on recorded footage or fingerprints, due to insufficient resources or inability to get a distinctive description. However, when quick video information is available they can respond.

<sup>14</sup> LSRA Cameras are connected by direct fiber cables to our server (not via the internet). Connecting via homeowner's internet can be slow & unreliable, and also has a challenge of guaranteeing privacy when networks are linked together (Port Forwarding and Mikrotik's provide only limited protections). Several experiments have been conducted over the years without any reliable success. Additionally, cameras on the LSRA system must be compatible make/models and also subject to setting adjustment by the LSRA to be consistent in our alerting protocols. The conclusion is that all of the trouble is not worth the cost & unreliability; so separate / dedicated cameras are installed at key locations.

<sup>15</sup> A.I. (Artificial Intelligence) is mistakenly assumed, and/or falsely advertised, to provide automatic setting adjustment or even detect human "shape" and suspicious activity. To-date, we have seen no software that genuinely provides this service. Therefore, painstaking manual set-up & re-testing is still required.

<sup>16</sup> Recent improvements in build-in camera software (aka Firmware) have made it such that advanced 3<sup>rd</sup> party software is now no longer required for typical home applications. However, the firmware requires proper set-up.

<sup>17</sup> Basic / Critical set-up can be achieved by either your Camera Installer or a Specialist recommended by your Camera Installer. However, it is best if the owner makes fine-tuning adjustment themselves - to get full value, by customizing to your unique landscape and risk tolerance versus burden of managing notifications / nuisance alarms. Regardless, neither Camera Installers nor Specialist can budget for continual adjustment and fine-tuning of camera settings; so, Owner should be prepared for paying for the additional consulting hours.

<sup>18</sup> Interconnection of the IT systems is the most challenging. By design, a networks' first priority is to protect itself from other networks, so forcing the linking together requires some technical skill to troubleshoot. Further, automatic updates to one software can break a critical link. Hence, why routine testing is so critical, so that troubleshooting can be prompted when a failure occurs.

<sup>19</sup> **Testing requires that the owner's themselves make the final physical tests, and not rely on others; so as to ensure the performance (and limitations) is understood.**

<sup>20</sup> Interconnectivity / Integration of CCTV systems with home-networks and notification software are NOT normally the responsibility of the Camera Seller / Installer in the industry.

<sup>21</sup> Experience has shown that the Off-Site Monitoring company have the most experience in knowing what settings get the best results from a Camera system.

<sup>22</sup> You can provide this info to your SSP, and that info will confidential/y appear on the company phone of the responder.