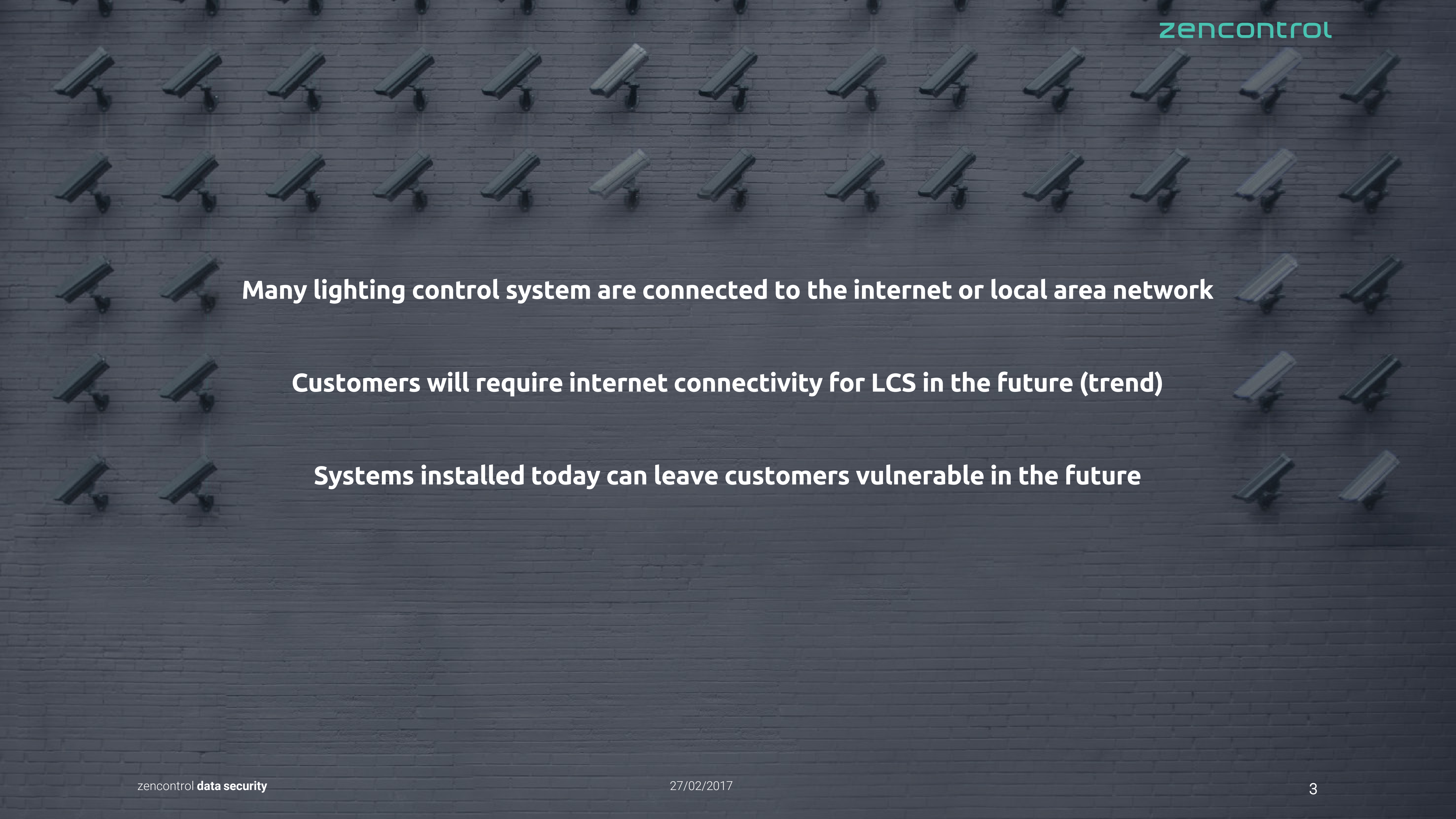
zencontrol

Data security



Many lighting control system are connected to the internet or local area network

Customers will require internet connectivity for LCS in the future (trend)

Systems installed today can leave customers vulnerable in the future

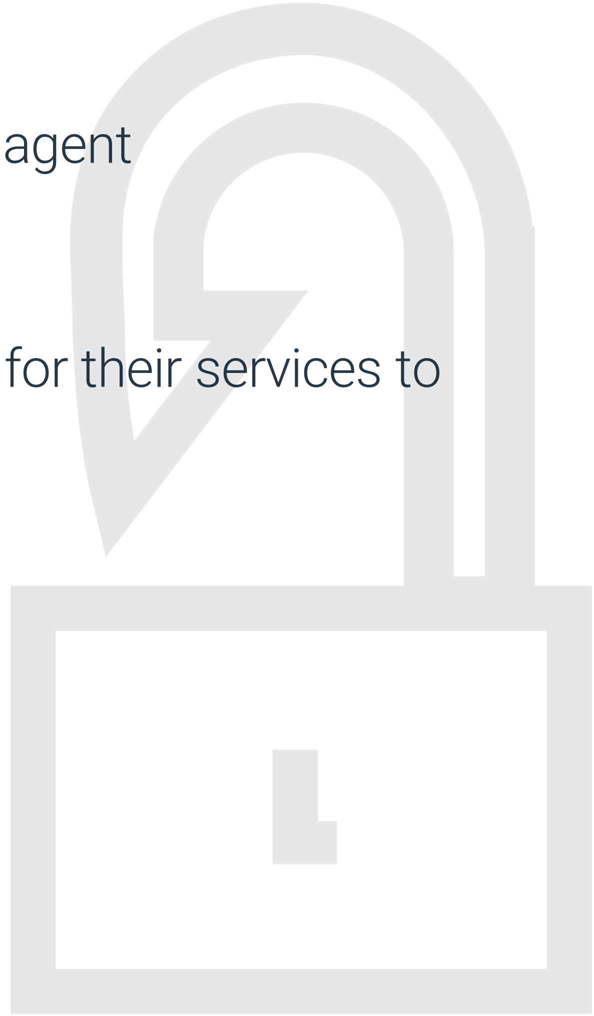
Data storage problems

Many current lighting control systems do not have a good recovery plan

- Data stored on a single low cost PC in the plant room
- No data redundancy
- No offsite backup
- Inadequate protection from virus, cryptolockers or ransomware
- No or limited PC maintenance
- Limited physical security - single password for all users
- Reports such as emergency test records could be lost, leaving users unable to prove testing was completed
    - No test reports could mean increased liability

Security of site information and setup

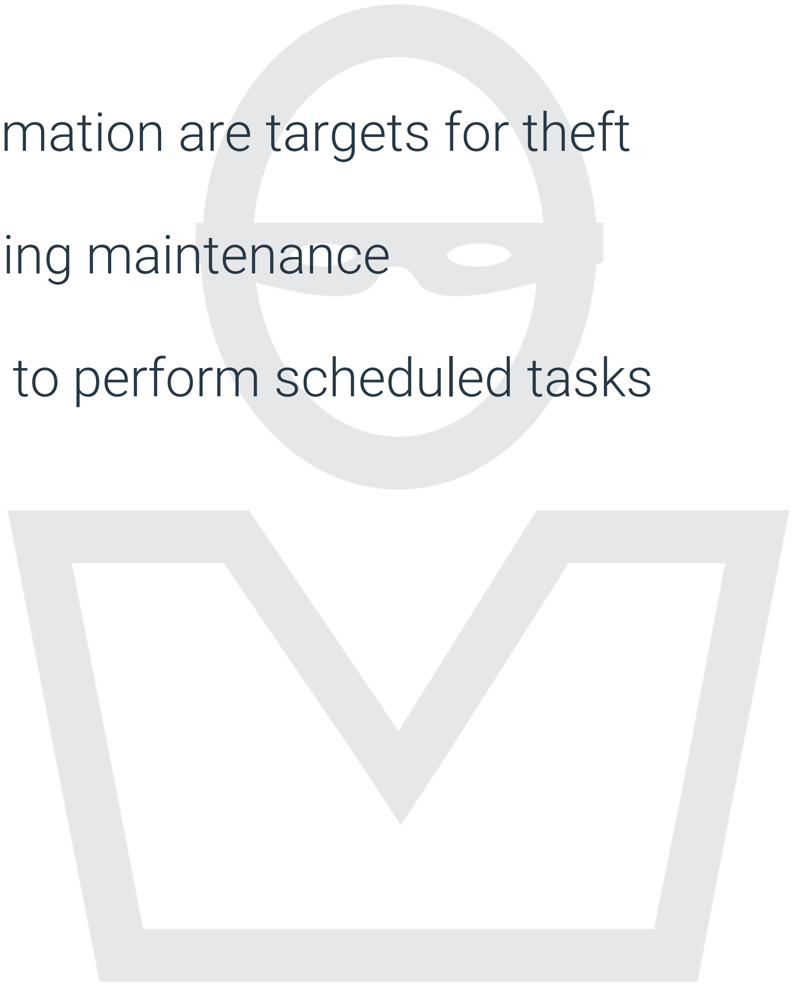
- Information or site files normally remain with the commissioning agent
- Agents may not have good security and data recovery plans
- Agents can keep setup files as their own IP, forcing clients to pay for their services to commission / change the site at a later date – locking client in



Malicious changes

- Current systems are often unprotected from malicious changes
- No protection from users changing the data incorrectly or maliciously
- No way to know when and where these changes occurred
- Users may be able to log onto the systems even when they leave the company
- Generic passwords and usernames used on most systems
- One password and login for most users

Theft



- PC systems which contain sensitive or important information are targets for theft
- PC systems are a target during construction and ongoing maintenance
- Many lighting control systems rely on the head-end pc to perform scheduled tasks

System security

- In most cases system software does not get upgraded over time
  - Any exploits or vulnerabilities are never patched, this includes both the OS software and the control system software
  - These systems can be used for botnets or illegal activities without the customer knowing

- Security does not increase over time
  - As more powerful attacks are developed the system is left more vulnerable
  - While the OS could be patched to increase security, the lighting control system is not (many use SQL or similar databases which need to be patched).

zencontrol data security

- zencontrol systems are stored on the cloud and follow standard best practice procedures
  - Data is backed up
  - Data is secured, both physically and digitally
  - Hardware maintenance is managed
  - Multiple fault tolerant servers
- Only approved personnel can access sensitive information
- Permission can be temporarily given to provide access without ongoing vulnerability
- Building managers can grant and revoke access to building areas and privileges
- Changes and users are logged and can be audited
- Incorrect or malicious changes can be identified and rolled back

zencontrol solutions

- Cloud based data storage means no need for local storage on PCs
- Head end PC is not required: less risk of theft
- zencontrol's system security is upgradeable, future exploits can be protected against
- All details of site setup is stored and can be accessed by any approved agent