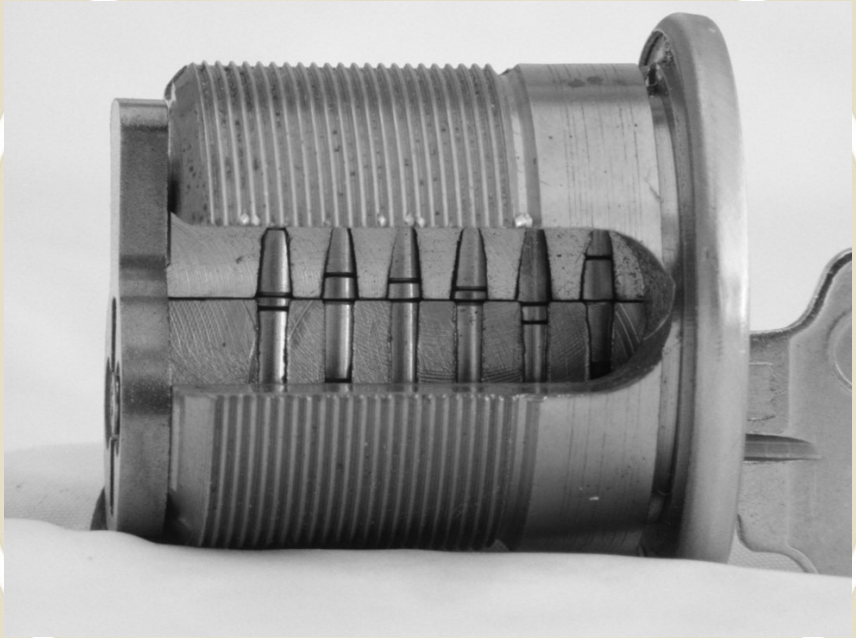
MASTER KEY SYSTEMS DATA: Security, Protection, Liability



SECURITY GUIDELINES FOR MANUFACTURERS, LOCKSMITHS, AND END-USERS

GOAL: Protection of master key system data from Unauthorized access, use, or compromise

INTRODUCTION TO MASTER KEY SYSTEMS

- MK SYSTEMS
  - Commercial and residential
  - Support organizational requirements
- PREVENT COMPROMISE:
  - Data security
  - Information confidentiality
  - Mechanical security
- GENERAL DATA PROTECTION REGULATION
  - Compliance requirements: manufacturers and distributors, individual personal data

MK SYSTEMS PROCESSES AND INTERFACES

- ISSUES OF DATA SECURITY AND LEGAL LIABILITY
- PROCESS STEPS:
  - Planning
  - Calculation
  - Production
  - Delivery
  - Installation
  - Maintenance

INDUSTRY NEEDS TO ADDRESS

- Industry-wide process for protection of Master Key System related data
  - Manufacturers
  - Distributors
  - Locksmiths

MECHANICAL LOCKS AND MASTER KEY SYSTEMS:

First line of defense in large and small facilities

- Conventional and High Security locks
- Systems designed by Manufacturers or Locksmiths
- Installed and maintained by locksmiths or end-users
- Security vulnerabilities
  - PHYSICAL SECURITY AND CONTROL ISSUES OF ASSETS
  - DATA SECURITY ISSUES
  - LIABILITY ISSUES

MASTER KEY SYSTEMS: The high value target

- Master keys and data are vulnerable
- Industry has not addressed MKS security issues
- Hackers and thieves and terrorists will target
- Global access can be obtained
- No audit trails
- Duplication and replication of keys possible
- Lack of control of a facility if compromised
- Systems cannot be easily changed

MKS COMPROMISE: RESULTS

- Protection of physical facilities
- Protection of people, assets, information
- Access to all areas
- Access to critical areas and facilities
- Breach of security by criminals and terrorists
- New techniques: can make compromise easier, especially 3D technology

COST OF A BREACH OF SECURITY

- Total rekey of a system
- Legal liability for damages by locksmith or manufacturer
- Criminal liability for failure to meet laws
- Cancellation of contracts
- Bad publicity
- Loss of certification

INDUSTRY STANDARDS AND GUIDELINES

- NO REAL STANDARDS FOR HANDLING MASTER KEY SYSTEM DATA
- Additional security measures will be required by:
  - Manufacturers
  - Regulators
  - Locksmiths
  - End-user customers
  - Public

WHY IMPORTANT?

- No consistency in rules protecting information and physical inventory
- Often easy to compromise MK systems through lack of controls at all levels
- MK systems provide the “keys to the kingdom”
- Public and facilities and assets can be at risk if a system is compromised
- Serious liability and security issues
  - Legal requirements
  - Contractual requirements
  - Certification issues
  - Protection of people, facilities, assets, information

INDUSTRY MUST DEVELOP GUIDELINES AND STANDARDS

- IF THE LOCK MANUFACTURERS AND SECURITY INDUSTRY DO NOT DEVELOP AND FOLLOW GUIDELINES, THEN FORMAL RULES WILL FOLLOW
  - Legal requirements
  - Regulatory rules
  - Privacy laws
  - Audits
  - End-users will demand accountability
  - General Data Protection Regulation 2018: Personal data at present

PAN-EUROPEAN GUIDELINES
MASTER KEY SYSTEMS DATA PROTECTION

OVERVIEW OF PROPOSED GUIDELINES
NINE CRITICAL AREAS

- Ordering and planning of cylinder systems
- Transmission of keying charts
- General data handling issues
- Calculation of MK systems
- Manufacturing of systems
- Shipments
- Locksmith key cutting
- Installation
- Lifetime management

1. ORDERING AND PLANNING

- Data to calculate and produce MKS
  - No personal information
  - Name, function, employee
  - Key markings

    No reference to function

    Door location or key holder

    Orders from only authorized customers

2. KEYING CHARTS AND DATA Mfg.+ Locksmith + Customer

- ELECTRONIC TRANSMISSION OR HARD COPY
  - Encryption and comm links
  - All systems encrypted:
  - Ordering and planning
  - Third party software
  - Email systems
- HARD COPY

  Registered mail or courrier

3. GENERAL DATA HANDLING

- Access management to server areas
- Storage in secure file systems
- PII authorization and GDPR compliant
- Backup files created and protected
- Access permissions constant review
- Security screened and vetted personnel with access to MKS calculations and software

4. CALCULATION OF MKS DATA

- Software from cylinder manufacturer or approved third party
- Must always follow manufacturer rules
- No reference to the location of the MKS

5. MANUFACTURING OF MKS

- Restricted access to production and assembly areas
- Access to data must be controlled
- After use of data, destroy, deleted or stored properly
- Test keys and incorrectly produced keys must be destroyed, no ID reference to system

6. SHIPMENT OF MK SYSTEMS

- Secure shipment of cards and master keys
  - Agreement whether sent together or separately
  - Always using registered mail or courier

7. LOCKSMITH KEY CUTTING

- Access limited to authorized personnel
- Protected key blanks
  - Store in secure and access controlled area
- Records about protected key blanks inventory:
  - Cut keys
  - Miss-cut keys
  - Disposed keys

8. MKS INSTALLATION

- Authorized personnel access: cylinders and keys
- Account for every key
- Hand-over audit to confirm order compliance
- Maintenance data to end-user
- Hand-over must be signed off by customer:
  - Security cards
  - Master keys and change keys

9. MKS DATA LIFETIME MANAGEMENT

- Record all changes:
  - System change and extensions
  - Replacement cylinders
  - Re-coding
  - Deleted cylinders
  - Additional keys
  - Deleted keys
  - System compromise

9A. SECURITY CARDS

- Identification of owner of MK system and allow reorders of cylinders, keys, copies
- Keep records of card issuance
  - New systems cards
  - Additional cards
  - Replacement cards
  - Lost cards

SPECIFIC ISSUES FOR LOCKSMITHS
ISSUES TO CONSIDER

- Regulatory
- Legal Liability
- Customer service
- Security

PROTECTION OF SYSTEMS AGAINST COMPROMISE

- POTENTIAL VULNERABILITIES
  - Key codes, keying lists for facilities
  - Remote and local computer access
  - Restricted key blanks
  - Who is authorized to obtain keys
  - Ordering new cylinders
  - Products in transit and shipment diversion
  - Inventory control
  - Audit systems for data, blanks, key machines

THE CRITICAL PLAYERS

- MANUFACTURERS
- LOCKSMITHS
- END-USERS

- LOCKSMITHS ARE THE MOST IMPORTANT
  - They are the gatekeeper
  - They are the most vulnerable to attack
  - Most are least equipped to deal with security issues

LOCKSMITHS: WHY MOST IMPORTANT

- Planning and ordering systems, or defining the system locally
- Responsible for receiving cylinders and keys
- Installation
- Keying, rekeying, adding to systems
- Cutting keys
- Storage of key blanks
- Maintain keying charts and data

LOCKSMITH SECURITY and MKS Does it exist?

- Can compromise an entire system
- They have all the critical information
- They have key blanks
- Responsible to verify credentials for restricted systems
- Ability to produce keys
- Ability to order new keys

INDUSTRY SECURITY GUIDELINES

- MUST ADDRESS CRITICAL ISSUES
  - Access to data and storage
  - Control and protection of information and inventory
  - Physical control of all elements that can compromise a system

  SECURITY CONCERNS

  PRIVACY ISSUES AND LEGISLATION

  REGULATORY ENFORCEMENT WILL FOLLOW

  COMPLY WITH CURRENT AND FUTURE USER SECURITY REQUIREMENTS

INDUSTRY GUIDELINES MUST ADDRESS

- Risk management and facilities security will require security audits
  - Manufacturer controls
  - Locksmith internal controls and procedures
  - End-user controls and procedures

  GOAL: THE PROTECTION OF:

  End-user facilities, assets, information

  Locksmiths

  Public

LOCKSMITH SECURITY AND MKS Required Elements

- Physical components: locks and keys
- System information: keying charts, code data
- Direct access to manufacturer via data links
- Computers and storage of information
- Mobile service vans for support and their security
- Interact with customers to produce restricted keys by authorized credentials

MANUFACTURERS AND LOCKSMITHS MUST TAKE LEAD

- IF THE INDUSTRY DOES NOT MOVE TO PROTECT ITSELF, REGULATORS WILL
- All manufactures will be involved
- Locksmith organizations must promote to protect the industry and customers
- Address protection of all elements
  - Design of systems
  - Implementation and installation of MKS
  - Support of systems

EVERYONE INVOLVED IN MKS
Responsibility for Security

- Of the process: Design, Protection of information, Implementation
- Of the result, and continued maintenance
- Legal liability
- Protect end-user system and facility
- Insure integrity of entire system

LIABILITY AND SECURITY ISSUES: Complex Issues

- DATA SECURITY: storage, access, transmission, deletion, updating
- PHYSICAL SECURITY: Locksmith, inventory, locks, keys, data, databases
- EMPLOYEE VETTING: Background, criminal history, access levels, audits, defining responsibility

UNDERSTAND SECURITY ISSUES AND RISKS

- STORAGE AND DATA ACCESS
- ORDERING NEW SYSTEMS VIA LINKS: EMAIL, FAX, INTERNET AND COMMUNICATION SECURITY
- WEB SITE DESIGN
- AUTHORIZATION LEVELS TO ORDER
- CUSTOMER DATA
- USE AND CONTROL OF TEST KEYS
- USE OF OEM PARTS PER CONTRACTS

PERSONNEL VETTING

- CRIMINAL HISTORY AND FINGERPRINT CHECK
- LICENSURE
- CREDIT HISTORY
- WORK HISTORY
- DRIVING RECORDS
- NON-DISCLOSURE AGREEMENTS
- TRADE SECRET AGREEMENTS
- BONDING

MORE SECURITY GUIDELINES

- COMPUTER SYSTEMS, ENCRYPTION
- SECURE DATA LINKS
- SECURE WEBSITES, EMAIL, PASSWORDS
- AUDIT TRAILS
- REMOTE ACCESS SECURITY
- THEFT OF COMPUTERS

LOCKSMITH PHYSICAL SECURITY

- SECURE PHYSICAL FACILITY
- ALARM SYSTREMS TO CENTRAL STATION AND CELLULAR
- HIGH SECURITY LOCKS
- SECURE SAFE OR VAULT FOR STORAGE
- COMPUTER BACKUPS
- DEFINE WHAT PII IS RETAINED AND HOW
- SMART CARD OR DONGLE SECURITY FOR COMPUTERS
- LOCKSMITH SERVICE VAN SECURITY

RISKS AND SECURITY GUIDELINES BY LOCKSMITH

- INFORMATION SECURITY
- HUMAN RESOURCE SECURITY: VETTING
- ASSET MANAGEMENT
- MEDIA HANDLING CONTROLS
- ACCESS CONTROL TO INFORMATION: FACILITIES, NETWORK ACCESS, AUTHORITY LEVELS, AUDITS, ACCESS RIGHTS, CRYPTO

LOCKSMITH PHYSICAL CONTROLS

- SECURE AREAS: UNAUTHORIZED ACCESS, DAMAGE, SECURE ENTRY CONTROLS
- PHYSICAL PROTECTION AGAINST: NATURAL DISASTERS, MALICIOUS ATTACKS, ACCIDENTS
- DELIVERY AND LOADING AREAS
- WORKING IN SECURE AREAS
- EQUIPMENT PROTECTION

RESPONSE TO SECURITY INCIDENTS

- QUICK, EFFECTIVE, ORDERLY
- REPORT AS REQUIRED
- REPORT SUSPECTED WEAKNESSES
- DOCUMENTED PROCEDURES

COMPLIANCE

- Legal and contractual requirements
- Applicable legislation
- Intellectual Property rights
- Protection of records
- Privacy and Protection of PII
- Use of crypto controls Independent review

QUESTIONS AND INPUT

- Are guidelines needed?
- Would guidelines be helpful and accepted?
- Do you think MKS data needs to be protected?
- How do you protect your systems?
- What suggestions do you have?
- Should the lock manufacturers or Locksmiths organizations develop standards
- Do you understand the potential liability involved?

MASTER KEY SYSTEM SECURITY

mwtobias@security.org