



SECURITY FACTS!!



A Quarterly Physical Security and Security Technology Newsletter

Vol. 3, No.4

In This Issue...

ASIS 46th Annual Seminar and Exhibits Begins 11 - 14 Sep 2000

Mas-Hamilton X-08 Lock is Different!!

Systems Approach to Security Matches Security Protection to Threat

Frequently-Asked Questions

Lock Talk ...

Commercial Products Can Protect Laptops Against Theft

Products are Available for Protecting Equipment Against Theft

*"The Doubting Thomas"
by John Fay*

ASIS 46TH ANNUAL SEMINAR AND EXHIBITS BEGINS 11- 14 SEP 2000

The American Society for Industrial Security (ASIS) produces the security industry's largest, most comprehensive educational program and exposition, attracting over 15,000 security practitioners and 1,000 exhibiting companies from around the world. With over 140 educational sessions spread over four days, the program addresses all facets of security management and practice. This year, the 46th Annual Seminar and Exhibits will be held in Orlando Florida from 11 to 14 September. You can register for either the exhibits only or the entire seminar online at <http://www.asisonline.org/seminar/seminar.html> or call Customer Service at (703) 519-6200 for an attendance package. Discounts on registration fees are available to all members.

This year, the attendees will be entertained by the satirical humor of "The Capitol Steps," a group of congressional staffers-turned comedians that spare no one, including Presidents, presidential wannabes, and other political headliners.

The keynote speaker on Tuesday, 12 September will be **Howard Fienman**, one of the country's foremost political reporters. He has covered every President since Jimmy Carter. He currently is Newsweek magazine's chief political correspondent and deputy bureau chief.

On Wednesday, 13 September the keynote speaker will be **Daniel Burrus**, one of the nation's leading science and technology forecasters. He will focus on how to turn a rapidly changing business environment into a competitive advantage by getting all members of an organization involved in creatively using the latest technology. Last but not least, the Closing Ceremony will feature entertainer Steve Allen, comedian, author, song writer, actor, and pianist.



The 140 educational sessions at the seminar will provide valuable presentations by security experts and practitioners on challenges that are faced daily. There will be lively discussions and hands-on demonstrations of :

- Workplace Violence
- Public/Private Law Enforcement Programs
- Information Security
- Terrorism
- Corporate Espionage
- Security Management Practices
- Career Development
- Computer Security
- Facility Design
- Executive Protection
- Personnel Screening
- Investigations
- Legal/Liability
- Emergency Planning

Other highlights of the seminar and exhibits include the ASIS foundation dinner, the ASIS Marketplace and Bookstore, the President's Reception, a Career Opportunity Center, and even a Spouse Program.

Make sure you don't miss this exceptional opportunity for quality education and networking that is unmatched in the security industry.

Mas-Hamilton X-08 Combination Lock is Different!!

The Mas-Hamilton X-08 combination lock was approved under FF-L-2740A in March 1999 and has been produced since October 1999. It is currently the only combination lock available on new GSA-approved security containers and vault doors used to protect classified information.

Lock outs on GSA-approved security containers and vault doors must be resolved using methods described in Federal Standard 809, if the container is going to go back in service for storage of classified information. These methods include:

- For a **red-label** Class 5 drawer, use a circular saw to cut the locking bolts.
- For a **red-label** Class 6 drawer, use a carbide-tipped holesaw to cut the locking bolts.
- For **red-label** doors (vault, or map and plan container) and any retrofitted black-label container, remove the dial and dial ring and drill into the lock

Traditional methods of drilling a lock cannot be used on the X-08 lock. There is no lever or lever screw to drill for. Consequently, Mas-Hamilton developed a way of opening the X-08 through a 1/4-inch hole with a special tool, designated as the X-08 Probe. A ten-step procedure is followed to retract the lock's bolt. The X-08 Probe (Part No. 501000) and opening procedures are available from Mas-Hamilton distributors.

NOTE

Federal Standard 809 is available on GSA's website:

<http://www.nfc.fss.gsa.gov/security>

Click on Technical Documents, then click on Standards, Specifications, etc., then scroll down to FED-STD-809.

GSA's website is also available by link from the DoD Lock Program website:

<http://locks.nfesc.navy.mil>


Another unique feature of the X-08 lock is the locked on by combination back cover (LOBC). A pin attaches the back cover to the lock case. To remove the back cover, the spring-loaded pin must be pulled at the same time the lock bolt is being retracted. This limits removal of the lock back cover to people who know the lock's combination. Attempting to remove the back cover with the pin in place will damage the lock.

There is a way of removing the pin when a container is unlocked, the



combination is lost, or the serial number is unknown. A template for drilling the cover lock pin is available from Mas-Hamilton distributors (Part No. 226000).

Remember, once the cover is removed, the lock serial number must be recorded before a new pin is installed and the lock is put back into service.

As with the Mas-Hamilton X-07 lock, the serial number of the X-08 can be used to reset a combination. Because of the LOBC feature, it is important that the serial number of the lock be recorded when the lock is installed. On a new container, already fitted with an X-08, the serial number should be recorded when the container is put into service. In X-08 locks, the serial number is the six-digit number on the capacitor (on the inside of the lock back cover). 

Systems Approach to Security Matches Security Protection to the Threat

The objective of a systems approach to security is to establish specific functional requirements for the design of security system elements. These requirements include: (1) The threat severity level the security system must protect against, (2) anticipated response time of the security guard force, and (3) any physical, functional, or budget constraints associated with the site or building that may affect the security system design.

Requirements must also take into account policies, measures, operations, and procedures contained in applicable military directives and instructions.

The term “*delay time*” refers to the amount of time it takes an adversary to penetrate a barrier or security system.

Delay time is normally acquired against intrusion by using balanced passive security measures, such as locks and barriers that impede intruders in their efforts to reach an asset. Appropriately designed and located barriers will effectively delay a forced entry attempt. In the case of forced entry, the delay must be sufficient to allow time for detection, assessment, and reaction by the security force.

The design of a forced entry delay system is based on the threat severity established for the asset. Forced entry threat severity is defined in terms of the relative effectiveness of the attack and the tools selected by an intruder to penetrate a barrier and gain entrance to a facility. The four basic threat severity levels are:

Low Level - Unlimited hand tools.

Medium Level - Unlimited hand tools and limited power tools.

High Level - Unlimited hand, power, and thermal tools.

Very High Level - Up to 50 pounds of explosives together with unlimited hand, power, and thermal tools.

As the severity levels proceeds from low to very high, the knowledge, skills, and abilities of the threat also

increase. Examples of the kinds of tools associated with the above threat levels are:

Hand Tools. Unlimited hand tools include any combination of high and low observable hand tools. High observable hand tools include the hammer, sledgehammer, cutting maul, shovel, pry axe, pick head axe, and fire axe. Low observable tools primarily used for covert entry include claw tool, carpenter’s saw, hacksaw, Kelly tool, bolt cutters, pliers, spanner wrench, tin snips, wrecking and pry bar, and wire cutters.

Power Tools. Unlimited power tools include electric (with power cord)-, gasoline- or air-powered circular saw; reciprocating saw; chain saw; saber saw; rotohammers (rotating jackhammer) and drills. Limited power tools can be the same as unlimited (circular, reciprocating, etc.), but are portable and the power source is self-contained. Hydraulic bolt cutters and rescue tools are included in the limited tool category.

Thermal Tools. Thermal tools include oxyacetylene, electric arc, or oxygen-fed cutting torches; burn bars; and rocket torches.

Explosives. Explosives include bulk TNT or plastic explosives, either alone or in combination with a flyer plate driven by the explosive to create a hole in a barrier.

Once the threat severity level has been established, the forced entry system must be designed to provide a balanced level of protection. As an example, the locking system must provide the same level of protection as the doors, walls, and windows included in the structure. Without this equivalency, the weakest link can be exploited by the intruder and the value of the delay system is effectively negated.

Contact the **DoD Lock Program** for help designing a security system. 



Frequently-Asked Questions

The answers you need are here!

Do I have to install the back cover locking pin when installing an X-08 or CDX-08 combination lock?


Yes, the back cover locking pin must be installed in order to meet the requirements of federal specification FF-L-2740A.

What do I do with the mechanical combination locks that I replaced with the X-07 or the X-08?

They can be destroyed, disposed of, or sent to your local Defense Reutilization and Marketing Service (DRMS).

NOTE! If you send them to DRMS **DO NOT** put them in the X-07 or X-08 boxes; they could wind up on the shelves for distribution.

Am I required to use the dial ring mounting plate when installing a CDX-07 or CDX-08 pedestrian door lock.

Yes, the mounting ensures the lock is mounted parallel to the dial ring and is required to ground the lock against electrostatic charge. 

SUBMIT YOUR QUESTIONS TO SECURITY FACTS NEWSLETTER

If you have questions or information on security equipment, storage of classified information or general security that you would like to share with our readers, please send them to the DoD Lock Program, 1100 23rd Avenue, Port Hueneme, CA 93043-4370. You can also e-mail them to any of the addresses contained in this Newsletter or call the Technical Support Hotline. If we use your question or comment in the Newsletter, you will receive a free T-shirt with the DoD Lock Program logo on the front. It is our way of thanking you for supporting our efforts.



lock talk...

Wondering What These Terms Mean?

American with Disabilities Act (ADA): A U.S. Federal law dealing with minimum standards of building accessibility and issues concerning individuals with disabilities.

Backset: The distance between the center of a cross-bore and the edge of a door.

Cylindrical Lockset: A bored lockset whose latch or bolt locking mechanism is contained in the portion installed through the cross bore.

Delay Time. The amount of time it takes an adversary to penetrate a barrier or security system.

Security Facts!!
Published by
NFESC



Using Appropriated Funds

The views and opinions expressed in this publication are not necessarily those of the Department of Defense.

Commercial Products Can Protect Laptops Against Theft

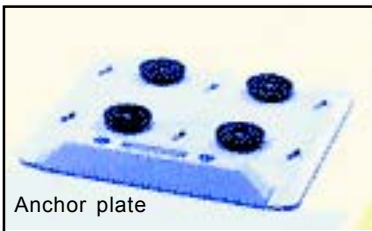
There are a number of security products available on the market that will provide a deterrent to theft of laptops. These products range from simple tags to sophisticated software systems. A few of the products available are:

- **Portable Alarms** - A cable is attached to the laptop by adhesive disks or to the security slot if it has one. The cable is connected to a portable alarm system powered by a 9-volt battery or the computer battery. The alarm sounds if the laptop is moved.



Portable alarm

- **Anchor Plates** - For laptops, an anchor plate is used to anchor the laptop when it is normally used in a primary location. The system is similar to those used for desktop computers.



Anchor plate

- **Laptop Security Stand** - This device is used to protect laptops that need to be mounted on a shelf, movable cart, or other work surface. It consists of a steel frame that secures the laptop in the open position. Nothing is physically attached to the laptop.



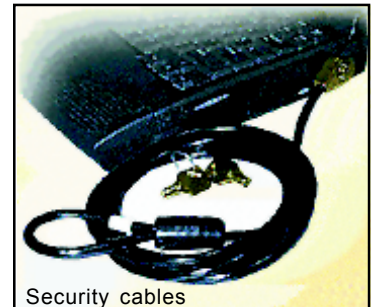
Laptop security stand

- **Laptop Vault** - This secure container for laptops is secured to the top of the work surface.



Laptop vault

- **Security Cables** - A cable is attached to the laptop by adhesive disks or to the security slot if it has one. The cable is padlocked to a piece of furniture.



Security cables

- **Tracking Software** - This software is downloaded onto the laptop in a hidden file. When a modem is attached, the software calls a monitoring center and, using caller ID, reveals the location of the laptop. The monitoring center, having been informed that the laptop has been stolen, reports the location to the local police. As an auxiliary benefit, this system will also log anywhere that a specific computer has been attached to a modem. The cost of this system is approximately \$100 for the software and \$60 to \$70/year for monitoring. A future enhancement could include global positioning to continually signal the location of the laptop without attaching a modem.

Products are Available for Protecting Office Equipment Against Theft

There are a number of security products available on the market that will provide a deterrent to theft of office equipment. These products range from simple tags to sophisticated fiber optic cable systems. Here is a partial list of products. While primarily marketed for the protection of computer systems, most products can also be used for the protection of other office equipment.

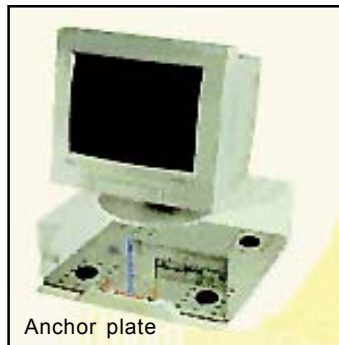
- **Security Cables** -

Cable systems are designed to protect single or multiple pieces of equipment through the installation of a fitting that is either bonded to the equipment and to the work surface using industrial strength adhesive or mechanical fasteners. A cable is then threaded through these fittings and secured with a padlock. Since the padlock and cable can both be easily cut, they are recommended only as a deterrent against a smash and grab threat or where an intrusion detection system is active.



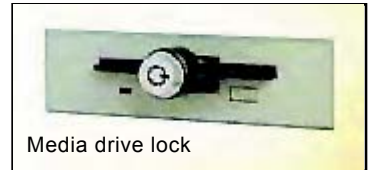
- **Anchor Plates** -

Anchor plates come in a number of styles and sizes. They consist of two plates, one bonded to the equipment and the other bonded to the desk. They have threaded metal bolts that hold the top plate to the bottom plate and a locking bar or interlocking plate design that keeps the equipment in place. These systems are more secure than cables because it takes more time to defeat them and there is a high probability of damaging the equipment during the removal process. They can only be used on flat, even surfaces. Peripherals are secured with cables attached to the anchor plate. The anchor plates can be removed without damaging the work surface when no longer needed.



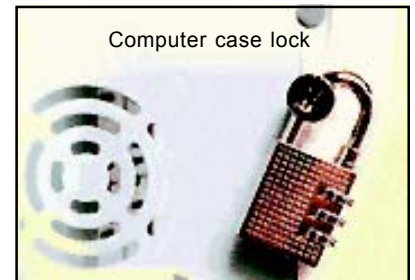
- **Media Drive Locks (floppy disks, CD, Zip drives, etc.)** -

These devices are inserted into the drive bay and locked in place with an integral key and lock system. They will not damage the floppy drive and they prevent anyone from using it. Devices are also available that prevent removal of the floppy disk. They are recommended only when access to the floppy drive is desirable or to prevent reboot of the computer from the floppy drive.



- **Computer Case Locks** -

These small locks are installed on the back of the CPU case to protect against tampering with the internal components of a computer.



- **Tamper-Resistant Plates** -

These are simple inexpensive tamper-resistant plates that are bar coded to allow for asset tracking. While they can be a deterrent to theft, they can be removed or covered to negate their effectiveness.



There are also a number of products available that provide higher levels of security for a computer and peripherals. They are:

- **Entrapment Systems** -

These systems consist of a heavy gage steel enclosure that



(Article continued on page 7)

(Continued from page 6)

interlocks with a bottom plate that adheres to the work surface. They are similar to the anchor plates in function but completely enclose the equipment.

- **Access Cards** - These systems are designed to work with Microsoft Windows or an NT computer password and use a proximity card to allow access to the computer.

These systems include the following features:

- Two-piece hardware and software access control card system.

- Single or dual factor authentication (card and PIN).

- Automatically locks the computer and blanks the screen when the card leaves the defined area and unlocks when the card re-enters the area.

- Programmable “active zone” from 1 to 50 feet works in virtually any office environment.

- Allows secure access by many users to one computer.

- Encrypted two-way communication prevents code grabbing and cloning of either the card key or the lock.

- Uses local configuration manager to administer settings and multiple key cards.

- Supplies event log and audit trail.



- Preserves work sessions and continues background tasks when computer is locked.
- Deploys incrementally to individual PCs or workgroups.
- Available for applications consisting of more than five computers.
- Easy to install and configure - full manufacturer’s support is available.

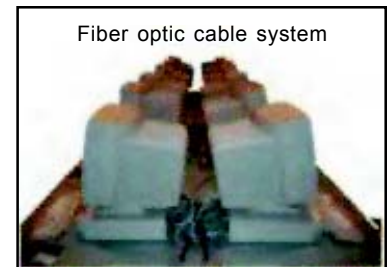
- **Equipment Tags** -

Security tags are attached to the equipment. The tag monitoring system is connected to a central alarm panel using network jacks or a wireless transmitter. Any attempt to remove the tag from the equipment or remove the equipment from the controlled area will activate an alarm.



- **Fiber Optic Cable Systems** -

These systems use a fiber optic cable to secure equipment. The cable is attached to the equipment and if the fiber cable is cut or disconnected, an alarm is activated. This system provides the added deterrent of an alarm.



FOR ASSISTANCE OR INFORMATION, CALL

DoD Lock Program Technical Support Hotline:

Comm: (805) 982-1212; DSN: 551-1212 (Leave a commercial number for return calls.)

Fax: 805) 982-2444 or DSN: 551-2444,
(805) 982-1553 or DSN: 551-1553,
(805) 982-1253 or DSN: 551-1253

E-mail: dodlock@nfesc.navy.mil

DoD Lock Program Technical Management Office

(805) 982-1567
DSN: 551-1567

Security Technology Project

(805) 982-1574, DSN: 551-1574

STP Training

(805) 982-1575, DSN: 551-1575

Drawer Head Replacement Program

(805) 982-1573, DSN: 551-1573

Security Engineering Division

(805) 982-1581, DSN: 551-1581

NOTE: If you are not a subscriber to the Security Facts Newsletter and would like your own copy or if you know someone who should be on our distribution list, please contact any of the individuals listed above. You can also send an e-mail message with your name, address, phone, FAX, DSN, and e-mail address along with your request to be added to our distribution list.

“The Doubting Thomas”

by John Fay

[This article is reproduced with the permission of John Fay, a security consultant in Atlanta Georgia. Mr. Fay is a staff columnist for Security Technology & Design (ST&D) Magazine. It first appeared in the June 2000 issue of ST&D.]

Several years ago at an annual security workshop I had the floor and referred to the corporation for which I worked at the time.

One of the attendees asked me how many employees were in the corporation. My answer was precise: “Eight thousand four hundred and eleven, and the reason I know that is because where I work there are 8,410 people who think they know more about security than I ever will.” That raised a laugh. Everyone in the room had had similar experiences.

A primary goal of a security leader is to instill in employees a confidence in the correctness of the organization’s security standards and practices. Security leaders do this even as they cope with disruptions like outsourcing, downsizing, mergers and acquisitions and technology shifts. For me, one of the most frustrating disruptions has been the doubting Thomas.

Skeptical, loud, and highly opinionated, the doubting Thomas is present at every level in an organization. By far, the doubting Thomas manager is the worst. He or she unfailingly shows up at every business meeting where security is on the agenda. The comments vary but are consistently negative: “The guard didn’t even look at me when I walked past the desk. That’s no way to run a ship.” Or, “CCTV at the loading dock? Whose stupid idea is that?” The capper is the advice. “If you want my opinion, here’s what you need to do...” The security leader’s reply, no matter how cogent it may be, will contain a faint ring of defensiveness that appears to validate the accusation. Some doubters are rarely seen or heard. They work within groups at line level and are out of the security leader’s sight and hearing. These doubters are not disinformation moles operating on behalf of a sinister adversary; they are ordinary employees who for one reason or another have a hang-up with security and express their dissatisfactions to co-workers. They divert attention from the positive aspects of security and contribute to the formation of a culture in which the security department is guilty until proven innocent. A doubter’s opinion can be particularly damaging when voiced before a large audience such as an employee town meeting.

The immediate inclination of the security leader in such a case is to wring the doubter’s neck. Effective as a good

throttling may be, it is not the politically correct reaction. What is needed is a careful plan to neutralize the doubter by conversion. The conversion is subtle and begins by finding out the why of the doubter’s negative attitude. The possibilities can include a dislike of the security leader personally or of authority figures in general, a past and unpleasant encounter with a security employee, a misunderstanding of how security fits into the total organization, etc.

If the security leader is to be effective at conversion, the doubters have to be identified. A good way to start is to solicit comments. The solicitation conduits can include telephone complaint line, electronic suggestion box, security chat room, e-mail fact-finding survey, written questionnaire, pull-off comment slips on coffee room bulletin boards and similar techniques. Department heads and supervisors can be excellent sources, especially for identifying the intractable doubters. These are employees so disenchanted with security that they refuse to respond to requests for comments.

After identifying the doubters, the security leader contacts each one personally and asks for a one-on-one meeting to exchange views. Many will accept; a few will be flattered. At the meeting, the security leader should be candid about purposes and not beat around the bush. The doubter can be asked to relate personal experiences with security, problems perceived and solutions in mind. The meeting is an opportunity also to get the security leader’s points across. Facts can be helpful but must be presented tactfully. The goal is to enlist the doubter as a supporter or minimize his or her negative impact. When the meeting is constructive, the security leader has a chance to establish a working relationship helpful in future situations. A proprietary interest on the part of the doubter is possible even when the input given has no security value. At the close of the meeting, the doubter should be thanked for being a contributor.

Converting skeptics is both difficult and essential. Like other management tasks, the more it is done, the better the doer becomes at it. It is a task fraught with failure because some skeptics are simply beyond conversion. Those who can be brought into the fold, even partially, are success stories.