

Managing Enterprise Cybersecurity

MIS 4596

Physical Security

Unit #18

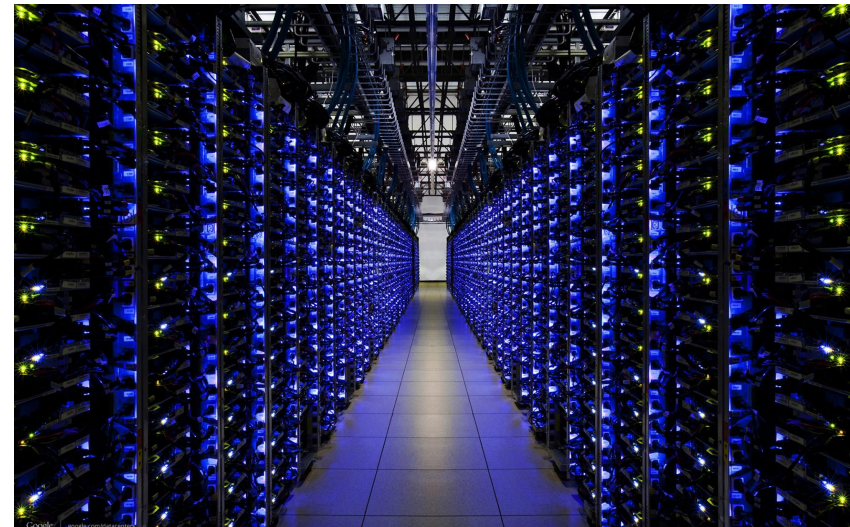
Agenda

- Vulnerabilities and sources of threats
- Physical control inventory baselines
- Perimeter security
- Media protection
- Media sanitization

Physical and Environmental (PE) Security

...encompasses protection of physical assets from damage, misuse, or theft

- **Physical security addresses**
 - ...mechanisms used to create secure areas around hardware
- **Environmental security addresses**
 - ...safety of assets from damage from environmental concerns



Sources of threats...

Materials

- ***Water*** – floods, leaks
- ***Chemicals and particulates*** - smoke, toxic materials, industrial pollution
- ***Organism*** - virus, bacteria, animal, insect
- ...

Water damage

– Damage from liquids (in general) can occur from many sources including:

- Leaking roofs
- Pipe breakage
- Firefighting efforts
- Spilled drinks
- Flooding
- Tsunamis



– Wet electrical equipment and computers are a lethal hazard

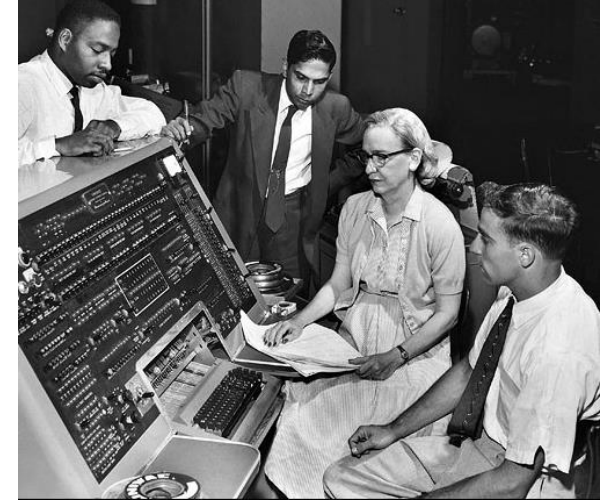
– **Preventative and detective controls** are necessary to make sure uncontrolled water does not destroy expensive assets or disrupt business operations

- **Water diversion** barriers to prevent water from entering sensitive areas
- **Water detection sensors and alarms** to detect presence of water and alert personnel in-time to prevent damage



First computer "bug"

Grace Hopper Ph.D. an American computer scientist and United States Navy rear admiral. Pioneer of computer programming, was the first to devise the theory of machine-independent programming languages, this theory was extended to create COBOL, an early high-level programming language still in use today



1947 Grace Murray Hopper records 'the first computer bug' in the Harvard Mark II computer's log book

- The problem was traced to a moth stuck between relay contacts in the computer:

"First actual case of bug being found"

- The engineers who found the moth were the first to literally "debug" a machine

Photo # NH 96566-KN (Color) First Computer "Bug", 1947


9/2
9/9

0800 Anchan started
1000 " stopped - anchan ✓ { 1.2700 9.037 847 025
1300 (033) MP-MC 2.130476415 9.037 846 995 convd
(033) PRO 2 2.130476415 4.615925059(-2)
convd 2.130676415

Relays 6-2 in 033 failed special speed test
in relay 10.000 test.

Relays changed

1100 Started Cosine Tape (Sine check)
1525 Started Multi Adder Test.

1545  Relay #70 Panel F
(moth) in relay.

First actual case of bug being found.

1630 Anchan started.
1700 closed down.

Relay 2145
Relay 2

Sources of threats...

Materials

- ***Water*** – floods, leaks
- ***Chemicals and particulates*** - smoke, toxic materials, industrial pollution
- ***Organism*** - virus, bacteria, animal, insect
- ...

Energy

- ***Fire***
- ***Explosion***
- ***Electricity, magnetism, radio wave anomalies***
- ...

Human – vandalism, sabotage, theft, terrorism, war

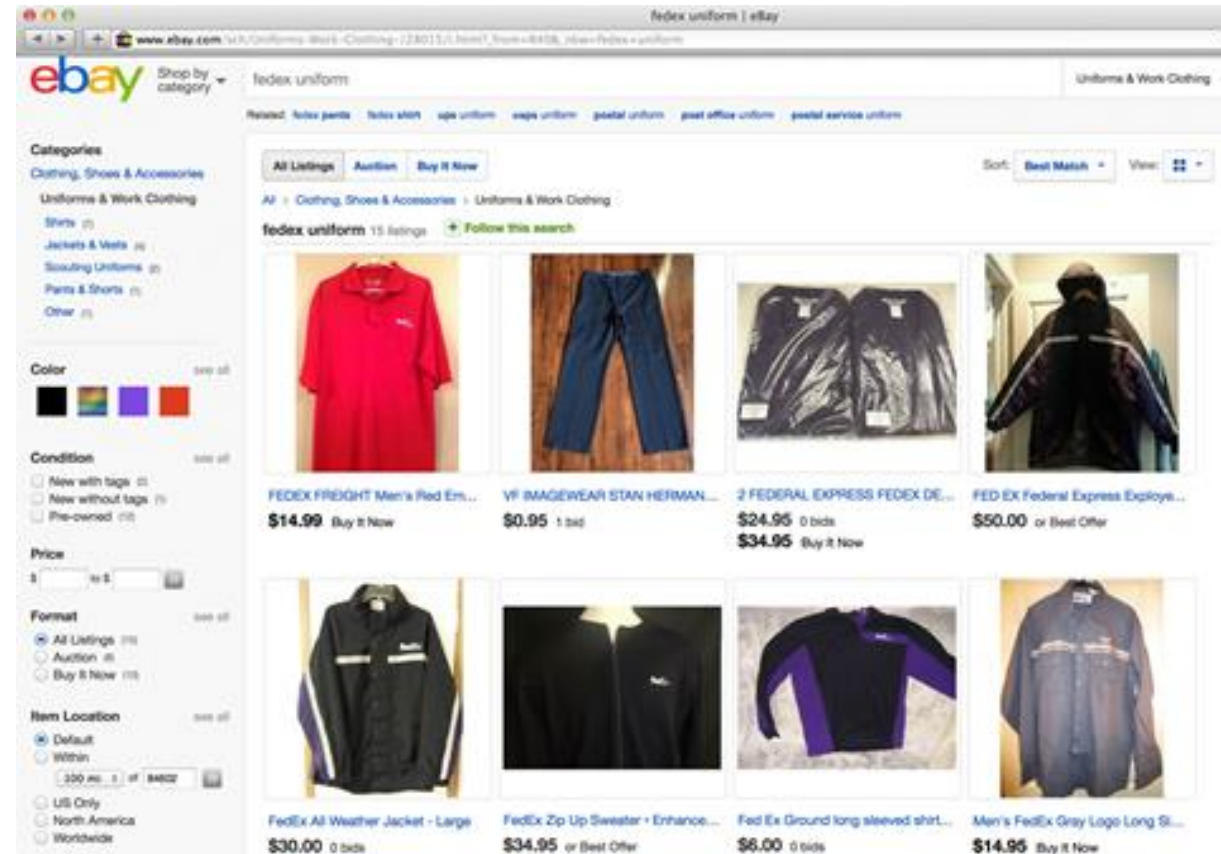
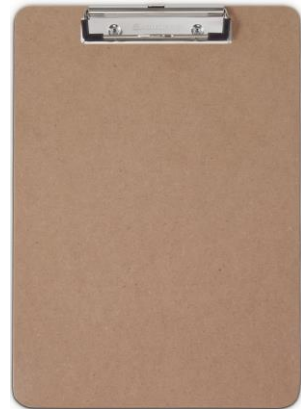
“Tailgating”, “Piggybacking” and Social Engineering



Social engineering

Are receptionists good at preventative security?

- **No**, their job is to help people feel welcome and guide them through the organization in an efficient way
- But intruders can get past guards with social engineering...







What could a hacker do,
once in a server room?

Physical access to an unlocked,
running system usually means
“game over!”





TrueCrypt Boot Loader 7.1

Keyboard Controls:

[Esc] Skip Authentication (Boot Manager)

Enter password: _

Cybersecurity controls

NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-53r5>

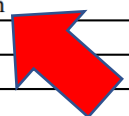
September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII



U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

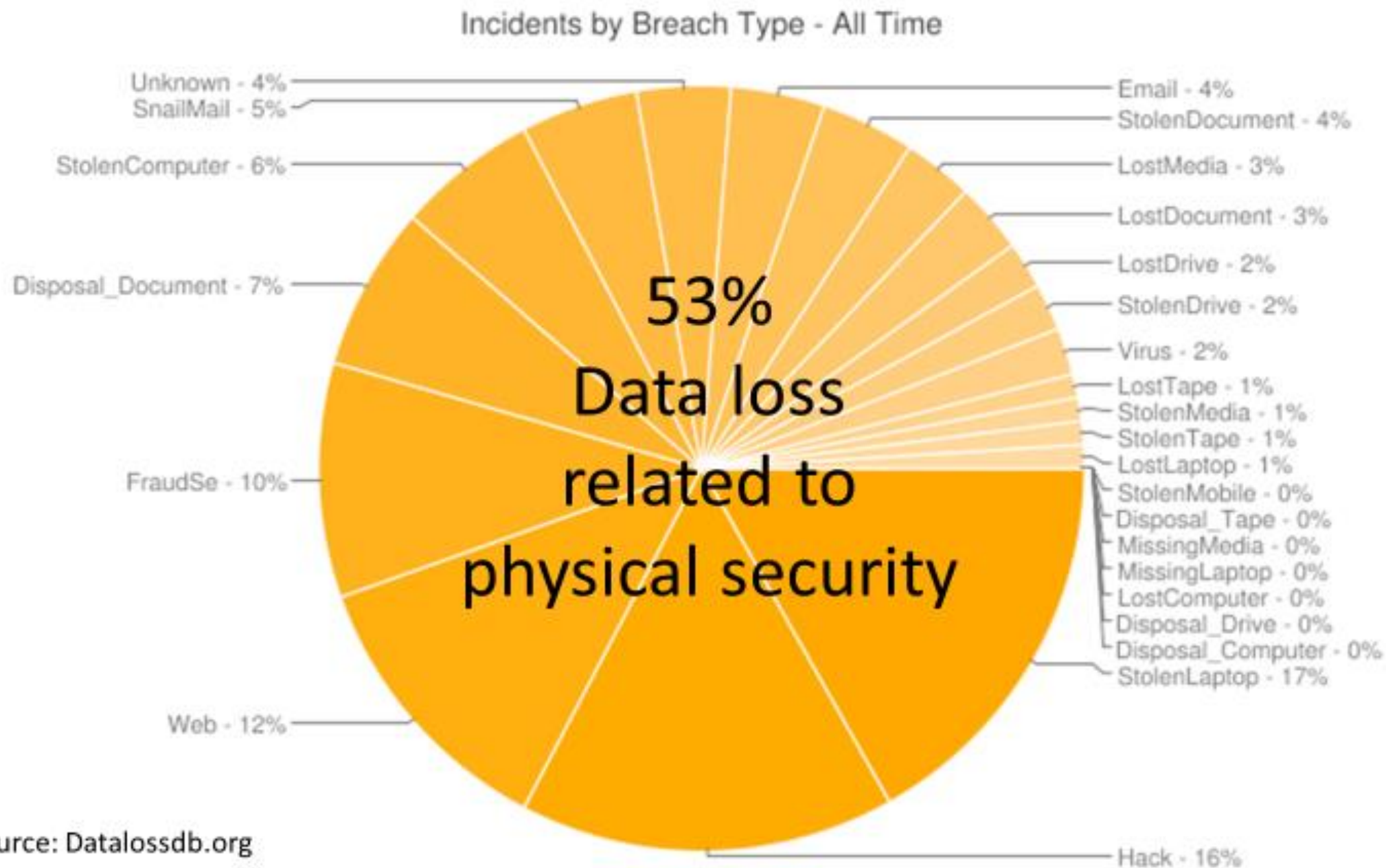
National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

CLASS	FAMILY
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration Management
Operational	Maintenance
Operational	System and Information Integrity
Operational	Media Protection
Operational	Incident Response
Operational	Awareness and Training
Technical	Identification and Authentication
Technical	Access Control
Technical	Audit and Accountability
Technical	System and Communications Protection



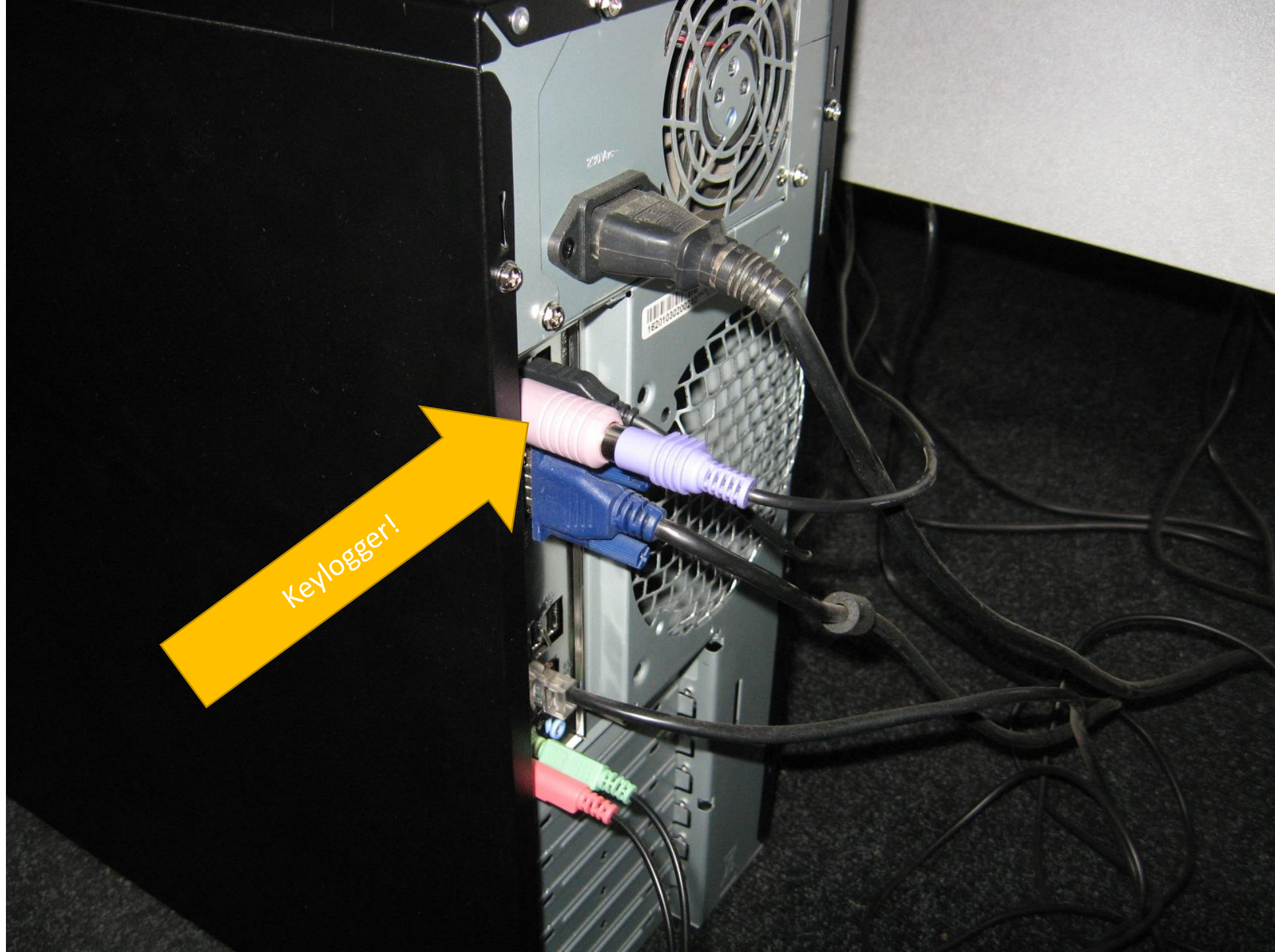
CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PE-1	Physical and Environmental Protection Policy and Procedures		X	X	X	X
PE-2	Physical Access Authorizations			X	X	X
PE-3	Physical Access Control			X	X	X
PE-3(1)	PHYSICAL ACCESS CONTROL INFORMATION SYSTEM ACCESS					X
PE-4	Access Control for Transmission Medium				X	X
PE-5	Access Control for Output Devices				X	X
PE-6	Monitoring Physical Access		X	X	X	X
PE-6(1)	MONITORING PHYSICAL ACCESS INTRUSION ALARMS / SURVEILLANCE EQUIPMENT		X		X	X
PE-6(2)	MONITORING PHYSICAL ACCESS AUTOMATED INTRUSION RECOGNITION / RESPONSES		X			
PE-6(3)	MONITORING PHYSICAL ACCESS VIDEO SURVEILLANCE		X			
PE-6(4)	MONITORING PHYSICAL ACCESS MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS		X			X
PE-7	Visitor Control	X	Incorporated into PE-2 and PE-3.			
PE-8	Visitor Access Records		X	X	X	X
PE-8(1)	VISITOR ACCESS RECORDS AUTOMATED RECORDS MAINTENANCE / REVIEW					X
PE-8(2)	VISITOR ACCESS RECORDS PHYSICAL ACCESS RECORDS	X	Incorporated into PE-2.			
PE-9	Power Equipment and Cabling				X	X
PE-10	Emergency Shutoff				X	X
PE-10(1)	EMERGENCY SHUTOFF ACCIDENTAL / UNAUTHORIZED ACTIVATION	X	Incorporated into PE-10.			
PE-11	Emergency Power				X	X
PE-11(1)	EMERGENCY POWER LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY					X
PE-12	Emergency Lighting			X	X	X
PE-13	Fire Protection			X	X	X
PE-13(1)	FIRE PROTECTION DETECTION DEVICES / SYSTEMS					X
PE-13(2)	FIRE PROTECTION SUPPRESSION DEVICES / SYSTEMS					X
PE-13(3)	FIRE PROTECTION AUTOMATIC FIRE SUPPRESSION				X	X
PE-15	Water Damage Protection			X	X	X
PE-15(1)	WATER DAMAGE PROTECTION AUTOMATION SUPPORT					X
PE-16	Delivery and Removal			X	X	X
PE-17	Alternate Work Site				X	X
PE-18	Location of Information System Components					X

Media theft



Key loggers

What's wrong
in this photo?



Keyloggers violate federal wiretapping laws



Keylogger!



Keylogger!

Key loggers



USB RUBBER DUCKY

\$49.99

Imagine you could walk up to a computer, plug in a seemingly innocent USB drive, and have it install a backdoor, exfiltrate documents, steal passwords or any number of pentest tasks.

All of these things can be done with many well crafted keystrokes. If you could just sit in front of this computer, with photographic memory and perfect typing accuracy, you could do all of these things in just a few minutes.

The USB Rubber Ducky does this in seconds. It violates the inherent trust computers have in humans by posing as a keyboard - and injecting keystrokes at superhuman speeds.

Since 2010 the USB Rubber Ducky has been a favorite among

“Dumpster diving”





Physical Security Control Types

Physical Controls

Perimeter security, fences, lighting, facility construction, keys and locks, access card and readers, ...

Administrative Controls

Facility selection, facility construction and management, personnel identity badges and controls, evacuation procedures, system shutdown procedures, fire suppression procedures, hardware failure procedures, bomb threat and lock down procedures,...

Technical Controls

Physical access control and monitoring system, intrusion detection and alarm system, fire detection and suppression system, uninterrupted power supply, heating / ventilation / air conditioning system (HVAC), disk mirroring, data backup,...

Agenda

- ✓ Vulnerabilities and sources of threats
- ✓ Physical control inventory baselines
 - Perimeter security
 - Media protection
 - Media sanitization

Perimeter Security



Perimeter security controls are used to prevent, detect and respond to unauthorized access to a facility

Perimeter Control

Fencing – different heights serve different purposes:

- 3 – 4 feet – deter casual trespassers
- 6 – 7 feet – deter general intruders
- 8 feet with barbed wire slanted at a 45° angle – deter more determined intruders

PIDAS – Perimeter Intrusion and Detection Assessment System

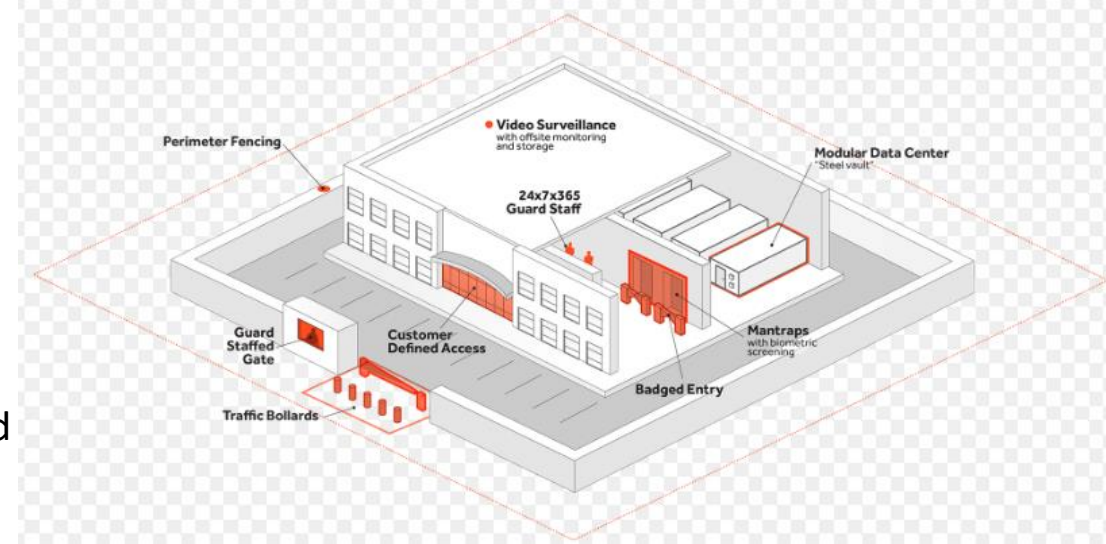
- Fencing system with mesh wire and passive cable vibration sensors
- Detects intruder approaching and damaging the fence (may generate many false alarms)

Bollards – Small round concrete pillars placed around a building

- Protects from damage by someone running a vehicle into the side of the building or getting too close for car-bomb

Lighting – Streetlights, floodlights or searchlights

- Good deterrents for unauthorized access and personnel safety
- National Institute of Standards and Technology (NIST) standard requires critical areas to be illuminated 8 feet in height with 2-foot candle power



Target Hardening

Complements natural access controls by using mechanical and/or operational controls:

- alarms, guards and receptionists
- visitor sign-in/sign-out procedures
- picture identification requirements,...



Restricted and work area security often

receive additional physical security controls beyond:

- *Key card access control systems*
- *Video surveillance*



Physical security controls for secure locations may also include:

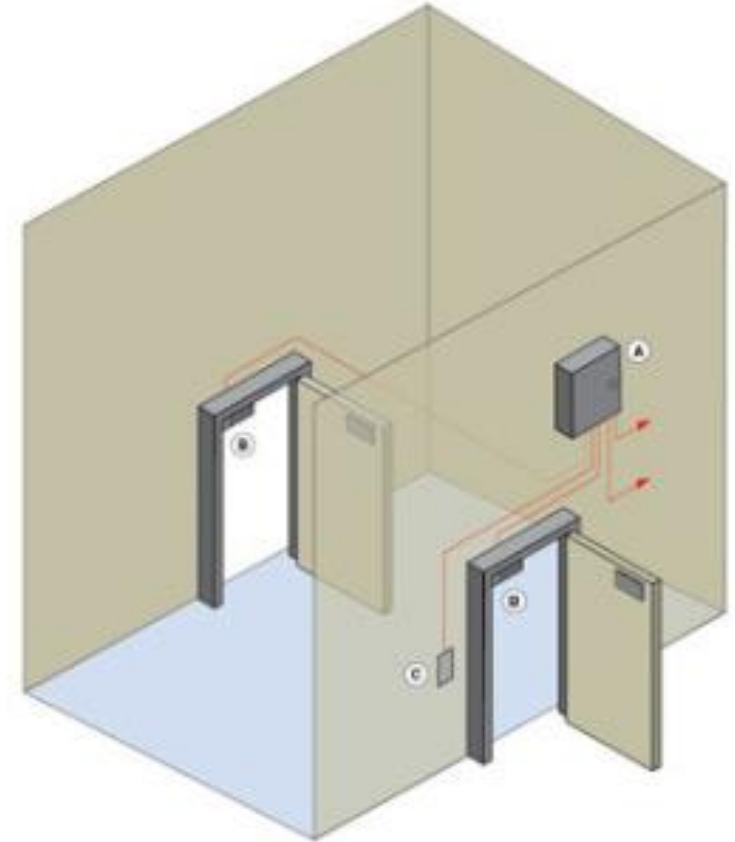
- **Multi-factor key card entry**
 - Bi-factor (or tri-factor): Key cards + PIN pad or biometric
- **Security guards (and guard dogs)**
 - At ingress/egress points to prevent unauthorized access, roaming facility alert for unauthorized personnel or activities, involved in capture of unauthorized personnel in a facility
- **Security wall and fences**
 - 1 or more to keep authorized personnel away from facilities
- **Security cameras and lighting**
 - Additional lighting to expose and deter would-be intruders
- **Security gates, crash gates, and bollards**
 - Limit the movement of vehicles near a facility to reduce vehicle-borne threats



Physical security controls for secure locations may also include:

Mantrap

- Made of two doors, one for entry, one for exit from the booth/ mantrap
 - When the first door is open, the second remains locked until the first one is closed and the individual inside the booth is cleared by a security operator monitoring this interlocking system

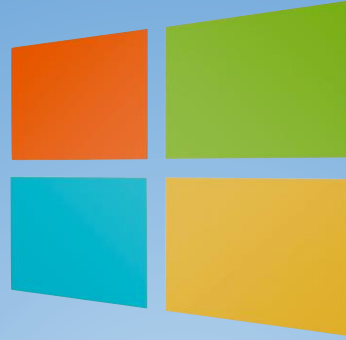




Agenda

- ✓ Vulnerabilities and sources of threats
- ✓ Physical control inventory baselines
- ✓ Perimeter security
 - Media protection
 - Media sanitization

Media protection



Bitlocker



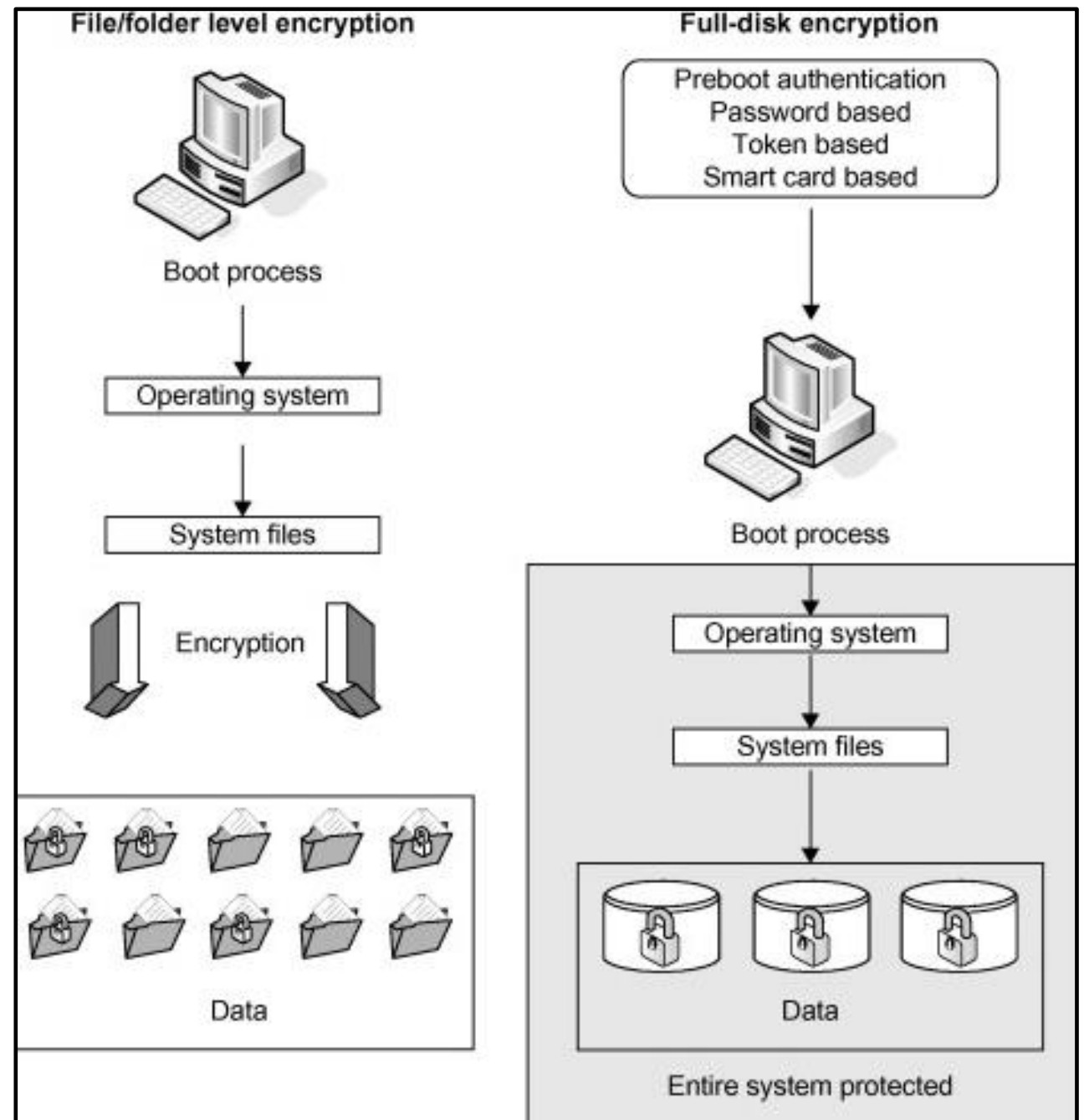
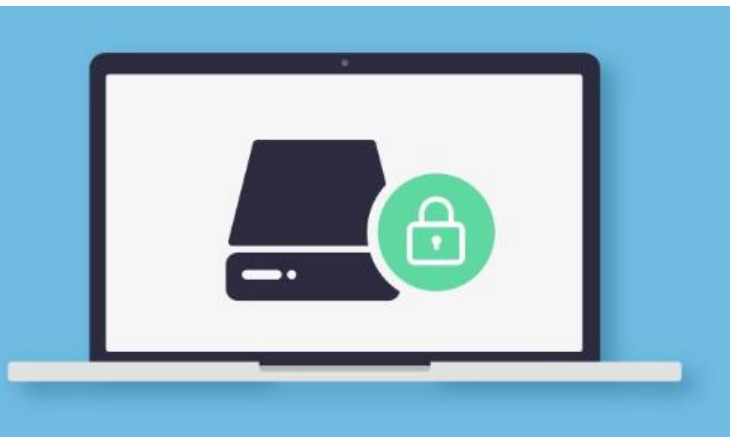
FileVault

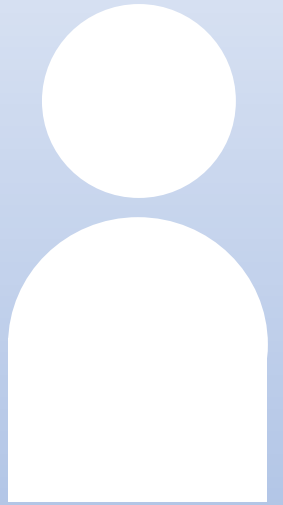


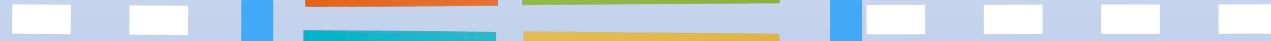
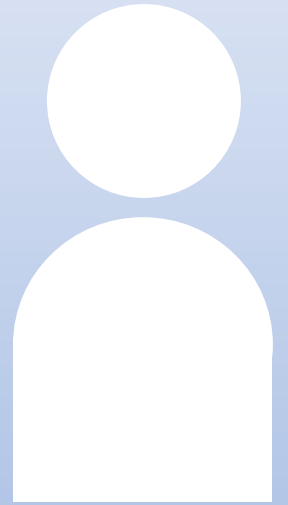
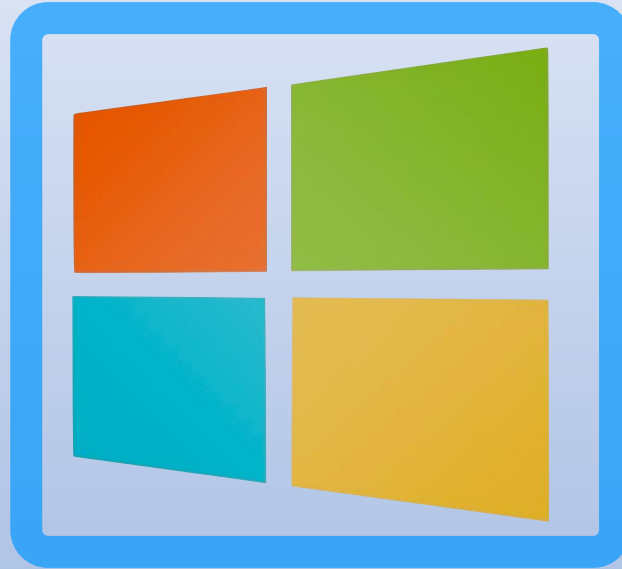
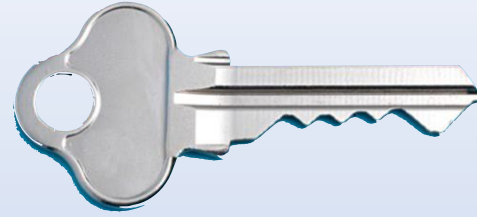
LUKS

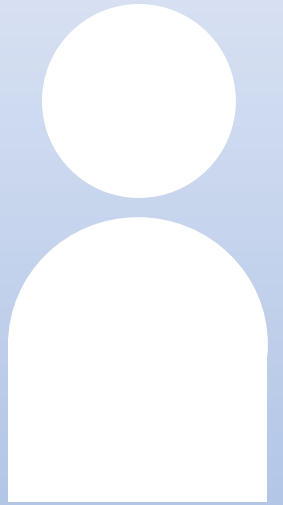
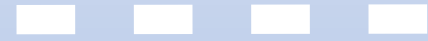
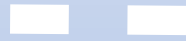
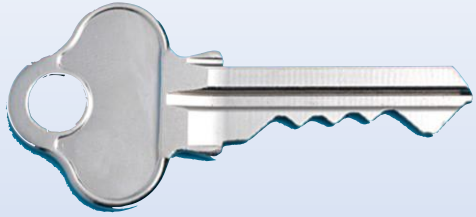
Full disk encryption

Uses disk encryption software or hardware to encrypt all data that goes on a disk or disk volume









Some disks have
built-in encryption

Agenda

- ✓ Vulnerabilities and sources of threats
- ✓ Physical control inventory baselines
- ✓ Perimeter security
- ✓ Media protection
- Media sanitization

Cybersecurity Controls

NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-53B>

NIST Special Publication 800-53
 Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-53r5>

September 2020
 INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII



U.S. Department of Commerce
 Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
 Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

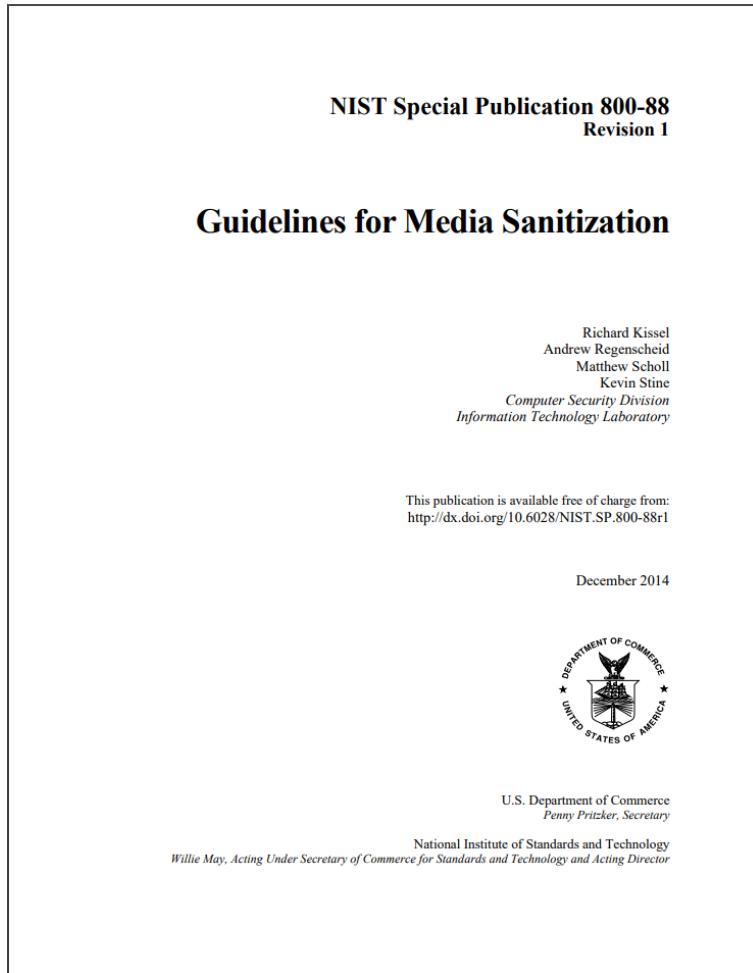
CLASS	FAMILY
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration Management
Operational	Maintenance
Operational	System and Information Integrity
Operational	Media Protection
Operational	Incident Response
Operational	Awareness and Training
Technical	Identification and Authentication
Technical	Access Control
Technical	Audit and Accountability
Technical	System and Communications Protection



CNTL NO.	CONTROL NAME <i>Control Enhancement Name</i>	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
MP-1	Media Protection Policy and Procedures		X	X	X	X
MP-2	Media Access			X	X	X
MP-2(1)	<i>MEDIA ACCESS AUTOMATED RESTRICTED ACCESS</i>	X	Incorporated into MP-4(2).			
MP-2(2)	<i>MEDIA ACCESS CRYPTOGRAPHIC PROTECTION</i>	X	Incorporated into SC-28(1).			
MP-3	Media Marking				X	X
MP-4	Media Storage				X	X
MP-4(1)	<i>MEDIA STORAGE CRYPTOGRAPHIC PROTECTION</i>	X	Incorporated into SC-28(1).			
MP-4(2)	<i>MEDIA STORAGE AUTOMATED RESTRICTED ACCESS</i>					
MP-5	Media Transport				X	X
MP-5(1)	<i>MEDIA TRANSPORT PROTECTION OUTSIDE OF CONTROLLED AREAS</i>	X	Incorporated into MP-5.			
MP-5(2)	<i>MEDIA TRANSPORT DOCUMENTATION OF ACTIVITIES</i>	X	Incorporated into MP-5.			
MP-5(3)	<i>MEDIA TRANSPORT CUSTODIANS</i>					
MP-5(4)	<i>MEDIA TRANSPORT CRYPTOGRAPHIC PROTECTION</i>				X	X
MP-6	Media Sanitization			X	X	X
MP-6(1)	<i>MEDIA SANITIZATION REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY</i>					X
MP-6(2)	<i>MEDIA SANITIZATION EQUIPMENT TESTING</i>					X
MP-6(3)	<i>MEDIA SANITIZATION NONDESTRUCTIVE TECHNIQUES</i>					X
MP-6(4)	<i>MEDIA SANITIZATION CONTROLLED UNCLASSIFIED INFORMATION</i>	X	Incorporated into MP-6.			
MP-6(5)	<i>MEDIA SANITIZATION CLASSIFIED INFORMATION</i>	X	Incorporated into MP-6.			
MP-6(6)	<i>MEDIA SANITIZATION MEDIA DESTRUCTION</i>	X	Incorporated into MP-6.			
MP-6(7)	<i>MEDIA SANITIZATION DUAL AUTHORIZATION</i>					
MP-6(8)	<i>MEDIA SANITIZATION REMOTE PURGING / WIPING OF INFORMATION</i>					
MP-7	Media Use			X	X	X
MP-7(1)	<i>MEDIA USE PROHIBIT USE WITHOUT OWNER</i>				X	X
MP-7(2)	<i>MEDIA USE PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA</i>					
MP-8	Media Downgrading					
MP-8(1)	<i>MEDIA DOWNGRADING DOCUMENTATION OF PROCESS</i>					
MP-8(2)	<i>MEDIA DOWNGRADING EQUIPMENT TESTING</i>					
MP-8(3)	<i>MEDIA DOWNGRADING CONTROLLED UNCLASSIFIED INFORMATION</i>					
MP-8(4)	<i>MEDIA DOWNGRADING CLASSIFIED INFORMATION</i>					



Media sanitization



Paper shredders have different levels of security, above:
Levels 1, 3, 6

Agenda

- ✓ Vulnerabilities and sources of threats
- ✓ Physical control inventory baselines
- ✓ Perimeter security
- ✓ Media protection
- ✓ Media sanitization