

Computer, Privacy, and Data Protection

Dr. Linda Wilbanks,
Chief Information Security Officer

Agenda

- What is a breach
- How does a breach occur
- What is at risk
- What you can and should do

What is a --

- **Security incident** – any event that compromised the confidentiality, integrity, or availability of an information asset
- **Data Breach** – An incident that resulted in confirmed disclosure, not just exposure, to an unauthorized party, often used interchangeably with data compromise

What Is a --

Privacy breach - when PII is lost or stolen, or is disclosed or otherwise exposed to unauthorized people for unauthorized purposes.

- This includes PII in any format, and whether or not it is a suspected or confirmed loss
- Examples of PII breaches:
 - PII left on the printer or scanner
 - PII e-mailed without encryption or other protection
 - PII mailed to the wrong recipient
 - PII stored on a stolen laptop or thumb drive
 - PII posted to a public-facing website, etc.

2015 Data Breach Investigations Report

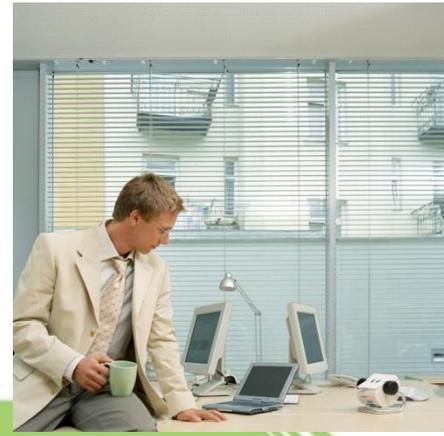
- 60% of cases, attackers are able to compromise an organization within minutes
- Nearly 50% of the people will open e-mails and click on phishing links within the first hour
- A campaign of just 10 e-mails yields a greater than 90% chance that at least one person click
- 99.9% of the exploited vulnerabilities had been compromised more than a year after the vulnerability was published (put patches in place!!)
- Half of the vulnerabilities were exploited within two weeks of posted. (patch quickly!!)
- Malware events focus on: financial services, insurance, retail, utilities, and education

Hacking Data Loss Examples:

- May 15, 2015 Penn State College of Engineering servers were hacked in two different intrusions, potential exposure for at least 18,000 people
 - October 1, 2014 City School District phishing attack allowed access to employees email accounts containing files with personally identifiable information, potential exposure 1,400
- <https://www.privacyrights.org/data-breach/new>
- **April 2015 Office of Personnel Management (OPM) was hacked and personally identifiable information for ALL federal employees (> 4 million) was assumed stolen**

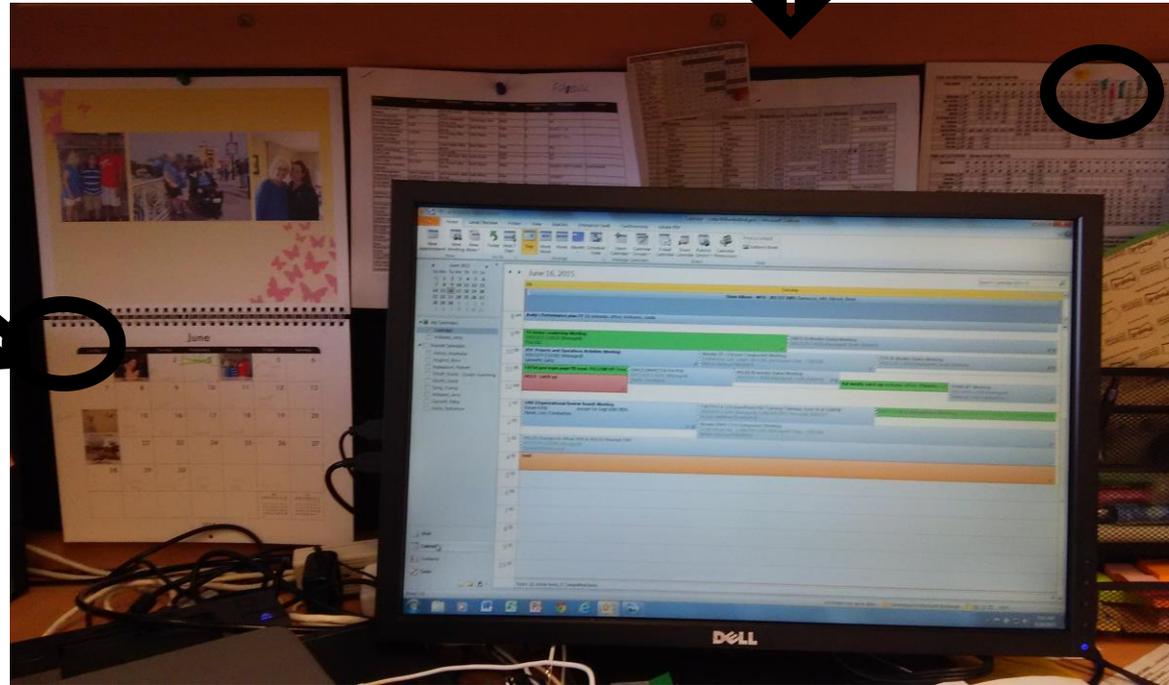
Who Perpetrated the Breaches?

- 86% perpetrated by outsiders
- 14% committed by insiders
- 1% business partners
- 7% multiple parties
- 19% state-affiliated actors



Your OFFICE tells ALL

Phone numbers
↓



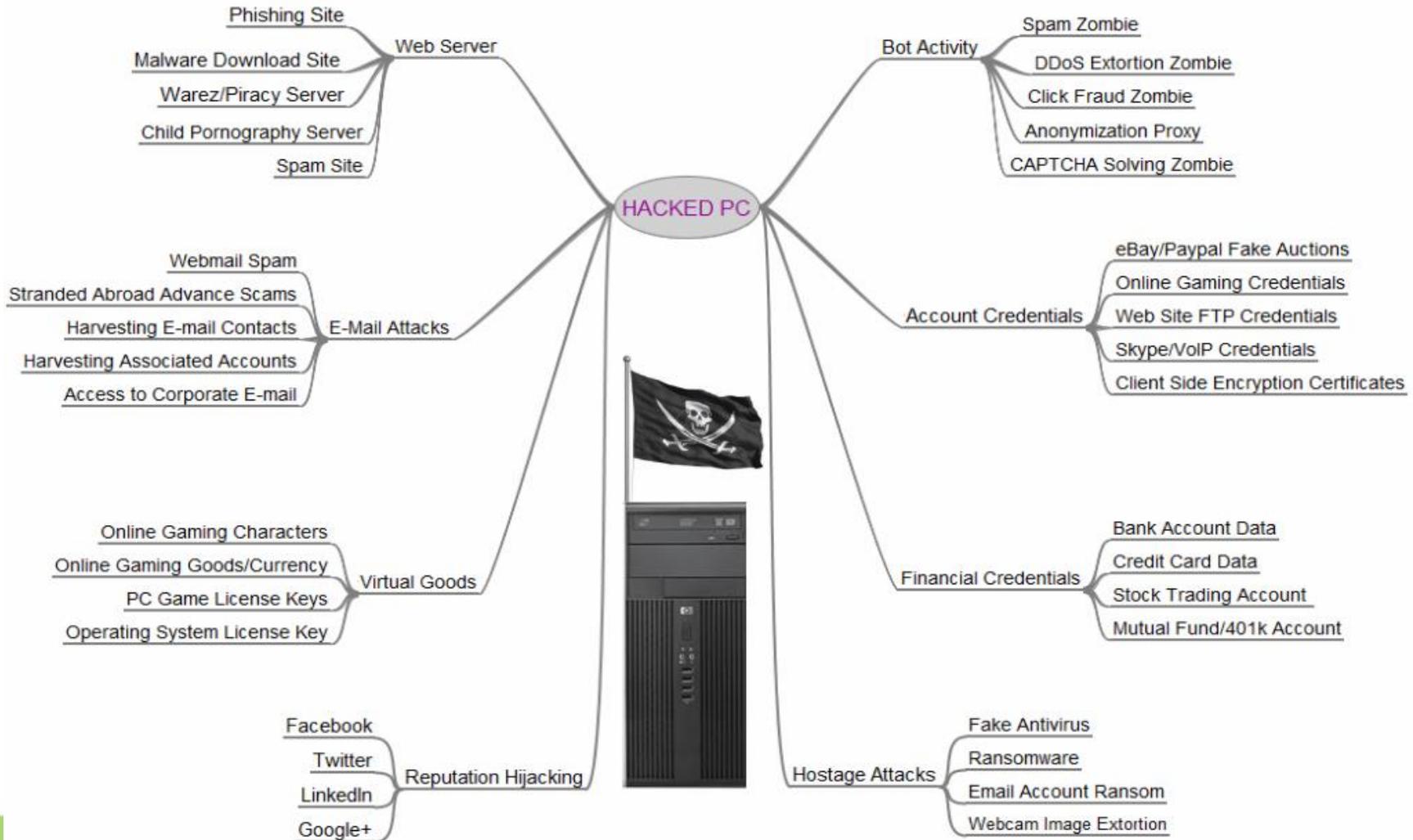
Passwords?
↘

Informative files
↓

Leave
information
↘



And Now: The \$100 Server



FSA Electronic Data Transfer Points

Department of Education

FSA Security follows Department policies and information roles up for Reporting

- Federal Partners – FSA Shares Data with:**
- Social Security Administration (SSA)
 - Internal Review Service (IRS)
 - Veterans Administration (VA)
 - Department of Justice (DOJ)
 - Department of Homeland Security (DHS)
 - Health & Human Services (HHS)



- FSA Major Applications and Interfaces**
- Business Solutions ~12
 - Supporting Applications ~6
 - Web Applications ~6
 - IT Infrastructure ~6



- Customers**
- Parents and Students
 - Schools and Universities



- FSA External Partners – Loan & Grant Disbursement and Management**
- Guarantee Agencies (GA) - 29
 - Private Collection Agencies (PCA) - 30
 - Title IV Servicers (TIVAS) - 5
 - Not for Profit (NFP) - 8



Breach Examples:

- July 8, 2010 Park Hill School District – employee downloaded files onto a hard drive, connected to their home network and the files went onto the internet with information of current and former students personnel files and social security numbers
- June 9, 2014 College of the Desert employee sent an attachment unencrypted to 78 employees containing personal information of college employees, impacting approximately 1,900 employees

Password cracking by security experts:

Six characters:	12 seconds
Seven characters:	5 minutes
Eight characters:	4 hours



What is at Risk



Networks – is someone on the network, capturing the data?



Data – is it being taken or altered?

Your Networks At Risk

- Current Student and Alumni Information
- Widely distributed networks
 - Admissions
 - Registrar's Office
 - Student Assistance
 - College Book Store
 - Health Clinic
 - Websites
- Hackers seek diverse information and diverse paths



Students (and Parents) Data at Risk

- Facebook = share everything (Security questions?)
- Very mobile = laptop, iPhone, iPad everywhere
- Very trusting = limited password usage, write passwords down
- Not organized = often do not track credit cards, “junk” mail
- High debt = attractive to foreign actors



Risk Mitigation

WHAT YOU CAN
and
SHOULD DO



It's NOT just IT's Problem

- YOU assume the risk for the loss of data
- IT protects the data to the identified risk level
- Data protection, breach prevention **MUST** be a joint operation for success



Establish Good Governance

- Create policies and procedures for protecting sensitive data and enforce penalties for noncompliance
- Develop a training and awareness program
- Publish rules of behavior – Make users sign a “confidentiality contract”
- Have a breach response plan that includes roles, responsibilities, timeframes, call trees, alternates, etc.
- Do you know how much PII you have, where it is stored (USB drives, CD-ROMS, etc.), who touches it, and why
- Map out your business process flows - follow the PII



Reduce Your Data Exposure

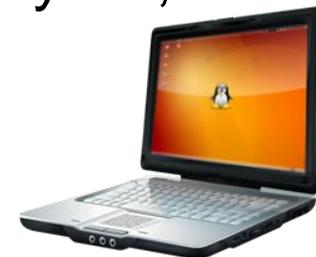
- Enforce a clean desk policy
- Conduct PII “amnesty” days (shred paper PII/eliminate PII from local and shared drives)
- Protect data at the endpoints
 - USB drives, paper, laptops, smartphones, printers
- Destroy your data securely
- Do not keep records forever
- Limit access to only those with a need to know
- Practice breach *prevention*
 - Analyze breaches from other organizations
 - Learn from their mistakes
 - Adjust your policies and procedures accordingly



- Please - **THINK** before you post/send/tweet!

Laptop risks:

- February 2015 University of Maine – A laptop was stolen with student roster information including social security numbers and grade data, potentially impacting 941 students
- July 2014 Orangeburg-Calhoun Technical College an unencrypted laptop was stolen from a staff member's office with personal information of approximately 20,000 current and former students and faculty members



<https://www.privacyrights.org/data-breach/new>

Tips to Safeguard PII

- **Minimize PII**

- Collect only PII that you are authorized to collect, and at the minimum level necessary
- Limit number of copies containing PII to the minimum needed

- **Secure PII**

- Store PII in an appropriate access-controlled environment
- Use fictional personal data for presentations or training
- Review documents for PII prior to posting
- Safeguard PII in any format
- Disclose PII only to those authorized



- **Safeguard the transfer of PII**

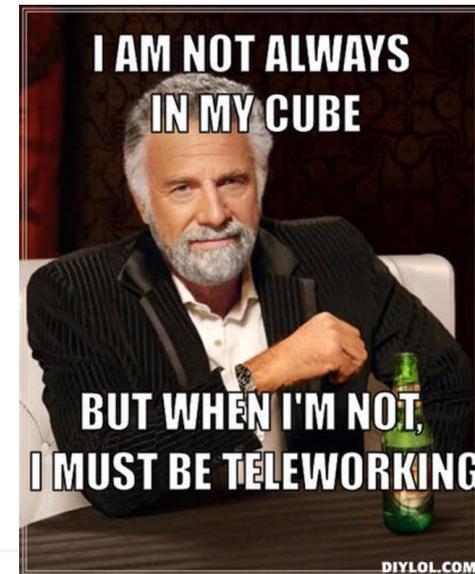
- Do not e-mail PII unless it is encrypted or in a password protected attachment
- Alert FAX recipients of incoming transmission
- Use services that provide tracking and confirmation of delivery when mailing

- **Dispose of PII Properly**

- Delete/dispose of PII at the end of its retention period or transfer it to the custody of an archives, as specified by its applicable records retention schedule

Teleworking Security

- Non-government computers or portable storage devices (e.g., a USB flash/thumb drive), should have ED-equivalent security controls (e.g., antivirus/malware, full disk encryption, session lock, strong passwords)
- If possible, do **NOT** copy data from the VPN to your hard drive, or to a removable storage device - If you must copy data, make sure the data is encrypted
- Keep your computer in a secure location; do not leave it unattended/unsecured
- If you are teleworking from a public location, make sure no-one else can see what is on your computer screen (consider a privacy screen)
- Encrypt PII/sensitive data when e-mailing such data (e.g., WinZip encryption)



Avoiding Identity Theft

Don't carry your SSN card with you!

- Request a drivers license number
- Shred sensitive information
- Only carry what you use
- Photo copy all cards in your wallet
- Select hard to guess PINs and passwords
- Don't leave mail sitting in an unprotected box
- Don't give out private information over the phone
- Order your credit reports
- Use caution when providing ANY sensitive information

The PERFECT Breach Response

- Auditor found PII on a public website
- Sent email to CISO and FSASOC
- FSA SOC verified PII
 - Incident report filed with ED
 - Removed site from web (verified)
 - Reviewed contractor logs to determine if information viewed by anyone (it was not)
 - Risk assessment low, incident closed (< 24 hours)
- CISO notified CIO and appropriate FSA & ED management & kept informed through out process

The Normal Breach Process

- Employee received PII for someone else
- Debated on what to do, shared it with friends and coworker for advise
- 2-3 days later sent to supervisor
- Supervisor did not see the email for a few days sent to friend in FSA technology office
- Friend decided to investigate, called person whose PII it was
- Person with PII data called FSA management who called CIO who called CIO

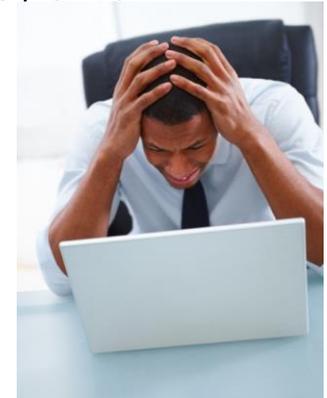
Who You Gonna Call

- Call your supervisor, the Help Desk, and Security and tell them exactly what is happening immediately
- Don't delete any files or turn off your system unless Security tells you to
- Don't send the files/data in question to anyone
- If you need advice or help, call your Federal Student Aid ISSO or the FSA Security Operations Center or the FSA CISO (Linda Wilbanks)



So, Once Again, All Together

- Only collect and use information that is **absolutely necessary**, and only share with those who absolutely need the information
- **“Review and reduce”**—inventory your PII and PII data flows, and look for ways to reduce PII
- Follow all Departmental **policies and procedures**
- **Think** before you hit the “send” button
- (**E-mail** is by far the #1 source of breaches)
- **“Scramble, don’t gamble”**- encrypt, encrypt, encrypt
- **Minimize** (or eliminate) the use of **portable storage devices**
- **Protect PII on paper**—enforce a clean desk policy, use secure shredding bins, locked cabinets, etc.



References



Privacy Rights Clearinghouse
Empowering Consumers. Protecting Privacy.

<https://www.privacyrights.org/>



<http://www.verizonenterprise.com/DBIR/2015/>



<http://securityintelligence.com/media/2014-cost-of-data-breach-study-ponemon/>

QUESTIONS?



Dr. Linda Wilbanks

Chief Information Security Officer
Federal Student Aid

Linda.Wilbanks@ed.gov

FSA Security Operations Center

202-377-4697