Data Security Best Practices & Reasonable Methods

September 2013

Mike Tassey
Technical Security Advisor
Privacy Technical Assistance Center (PTAC)

http://ptac.ed.gov/
E-mail: PrivacyTA@ed.gov
Phone: 855-249-3072

FERPA and Data Security

- Unlike HIPAA and other similar federal regulations, FERPA does not require specific security controls
- This provides room for innovation, but also heaps more responsibility on the community to protect the privacy and security of student data
- As educators we have student data in many places, including our own machine / mobile devices
- It's up to us to ensure that we take the necessary security measures to protect student data

What is data security?

What is data security?

There is no route to Secureville!

- It is **not** a destination
- It is **never** 100%
- It does **not** come in a box

  (no matter what the vendor says)
- It is **not** a paper exercise
- It does **not** run on autopilot
- It does **not** stop with compliance

What is data security?

Data security is about risk management.

Its hardware, software, policy & people working together to reduce the risk to an organization's systems and data.

Data security is everyone's responsibility.

Understanding risk

Balancing Risk and Resources

- Risk = Vulnerability + Threat
  - Assessment of your own weaknesses
  - Understanding of the threats
  - Organizational understanding of how much risk is "too much"
- Concentrate resources where the risk is greatest
- Reduce risk by applying security controls
- This is not a one time deal, it's a continuous process

Understanding risk

Who are the bad guys?

Cybercriminals

Nation States

Hacktivists

Understanding the attacks

Attackers have lots of options:

- Using malicious web sites to distribute malware or execute client-side attacks
- Attacking web applications to gain access to back-end data
- Exploiting Wi-Fi through poorly secured access points or through spoofing
- Social engineering through email, the phone or in person
- Malicious applications for your smartphone
- Dumpster diving or physical theft

Understanding the attacks

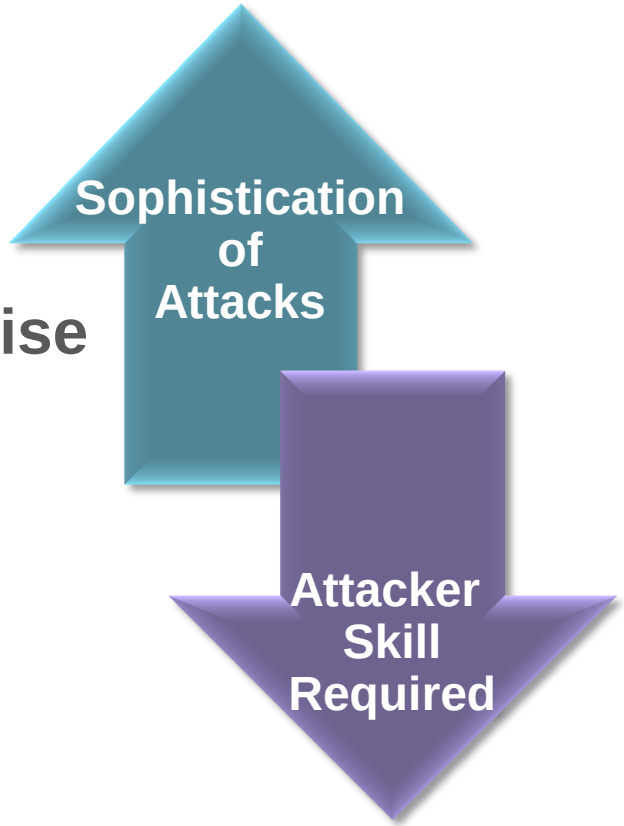
Attack Surface is Growing

- Software is becoming larger and sharing more code each year
- Wider variety of devices and associated software
- Explosion of mobile technologies and BYOD is changing the concept of “system boundary”
- The shift to a digital economy means we expose more of our business to the internet

Understanding the attacks

Its getting easier to be a bad guy

- Adoption of the Digital Economy
- Increasing Complexity in the Enterprise
- Still Developing Flawed Code
- Free & Open Source Tools
- Automation of Attacks
- Internet Collaboration



Security Best Practices & Reasonable Methods

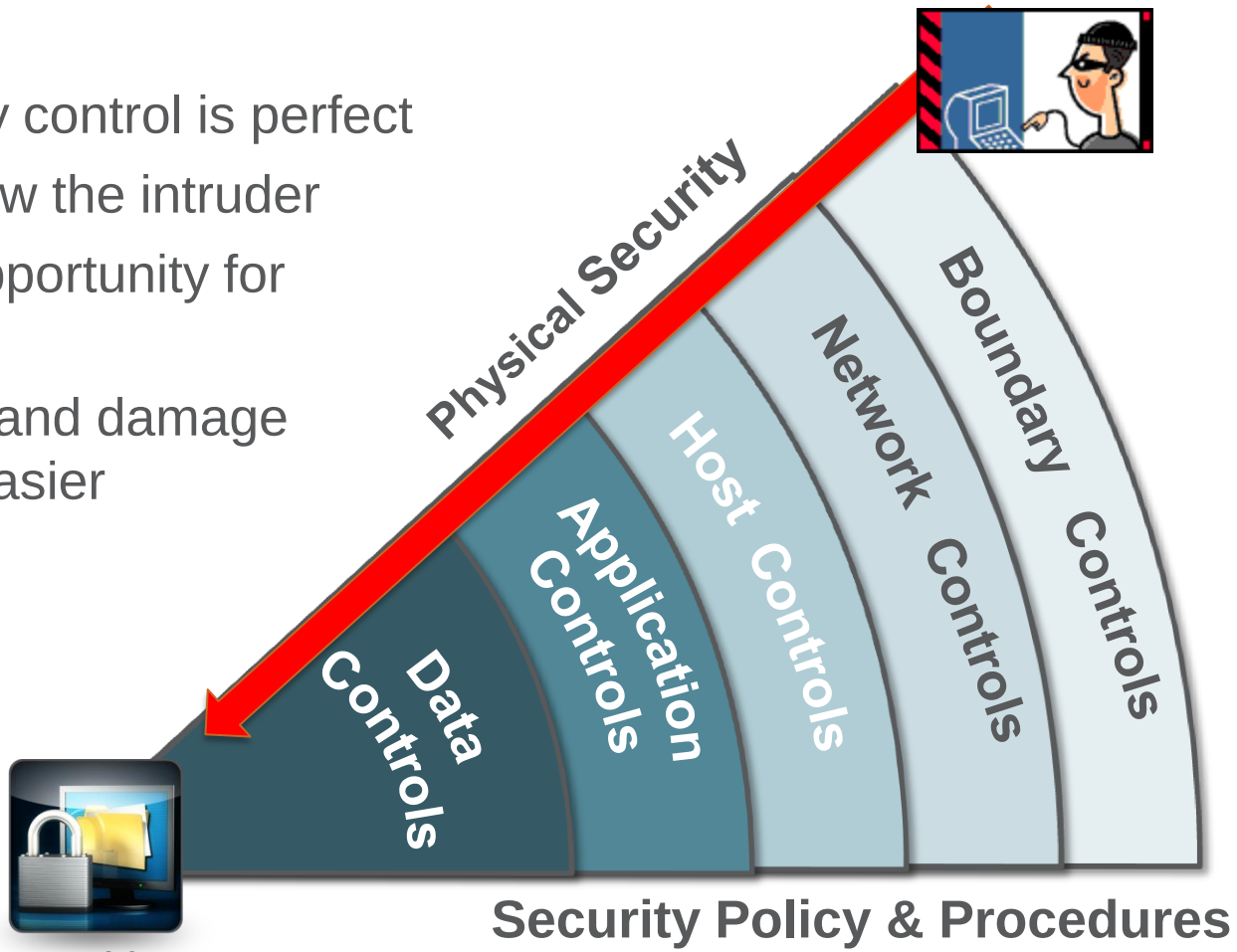
> Technology is where the rubber meets the road

- Technology is a tool to help us implement a data security strategy
- In order to be effective, the tools must be selected carefully, configured properly, managed well and evaluated often
- Automation can help you make the most of limited resources, but too much can leave blind spots
- Don’t implement what you can’t monitor

Security Best Practices & Reasonable Methods

Employ a "Defense In Depth" Strategy

- No single security control is perfect
- Layers trap or slow the intruder
- Provides more opportunity for detection
- Makes response and damage control faster & easier



Security Best Practices & Reasonable Methods

Encrypt Your Sensitive Data

- Where practical, employ strong encryption to protect data at rest and in motion
- Federal Information Processing Standard 140-2 provides recommendations on employing a wide variety of encryption schemes
- Implement SSL/TLS to protect web sessions both internally and externally
- Don’t implement what you can’t monitor

Using encryption can help prevent “man-in-the-middle attacks” and reduce the risk of data loss through lost or stolen equipment

Security Best Practices & Reasonable Methods

Network Architecture

- Implement a rich network topology to create security enclaves within your environment
- Keep desktops and personal / mobile devices separate from each other and production environments
- Understand which ports, protocols and services are used within your environment and restrict where it makes sense
- Tightly control changes to the network topology and boundary rules for both ingress and egress

Security Best Practices & Reasonable Methods

Implement a Baseline

- Create a list of approved software, hardware and configurations in your environment
- Use the baseline as a tool to evaluate whether the reality of your environment meshes with your organizational policy
- The baseline helps you control your enterprise by giving you a snapshot to refer back to as your systems change and grow, if there is divergence then there may be a need to either enforce the standard or to evaluate the need for a change to the baseline
- Either way, you cannot protect something that you don't understand and can't quantify

Security Best Practices & Reasonable Methods

> Data Security is as much about culture as it is about technology

- Top down approach to security is foundational to creating a “culture of security”
- Data security doesn’t start and end with IT, it starts with your users, developers and executives
- Training & awareness is still the best bang for the buck in data security

Security Best Practices & Reasonable Methods

Train Your Users and Staff

- All users should read and sign an Acceptable Use Policy (AUP) which establishes rules governing the use of organizational computer resources
- Consider also requiring users to agree to addendums to the AUP relating to confidentiality and data use requirements
- Implement a security awareness training program which provides users and admins alike with a basic understanding of data security and their responsibilities to protect data
- Build a “culture of security” in your organization by encouraging users to be actively involved in the security of sensitive data they work with

Remember - *A trained and engaged user base is the most effective weapon to detect and counter malicious attacks.*

Security Best Practices & Reasonable Methods

Have an Incident Response Plan

- You will have a breach or security incident… it isn't a question of "IF" it's a question of "WHEN"
- Before a breach happens, you should have identified a plan for responding
- Identify in writing an incident response team and set aside the resources necessary to appropriately deal with it, identifying the stakeholders and lines of communication
- The law varies, so work closely with legal counsel to determine what your legal responsibilities are in terms of notifications and incident handling
- PTAC has resources like our "Data Breach Response Checklist" available at our website http://ptac.ed.gov/

Security Best Practices & Reasonable Methods

Create a Configuration Control Board

- Chaired by a management executive
- Chartered to manage and control changes to the enterprise and evaluating and approving changes to the system
- Consists of representatives from executive leadership, IT, production or development, etc.
- Major changes to the enterprise are presented to the CCB, evaluated to assess risks and benefits and voted on by the members
- The CCB process encourages consensus and requires that changes be considered thoroughly before implementation and before money is spent

Security Best Practices & Reasonable Methods

Pro Tips for the Enterprise:

- Set security policy that defines expectations, metrics and roles & responsibilities
- Educate yourself on the threat and assess your risk exposure
- Create a security training and awareness program, make it fun
- Don’t run out and buy a bunch of technology, make what your already have work better
- Know where the most important “stuff” is
- Identify gaps and deploy mitigating controls to reduce the risk to acceptable level
- Test your security and response capability annually
- Require third-party service providers to handle your data with at least the same level of protection as you provide

Security Best Practices & Reasonable Methods

Tips for Protecting Yourself:

- Refrain from using untrusted networks for sensitive work
- If you don't need it, get rid of it
- When sending out sensitive info, consider using encryption
- Keep your OS, anti-virus and third party software fully patched and updated
- Examine the terms of service and privacy policy of free services you use
- Be wary of unsolicited emails or attachments
- Use strong and complex passwords, apply passcodes to your mobile devices
- If something doesn't feel right… report it.

ED/PTAC Resources available

- Data Sharing
  - Data Sharing Agreement Checklist
  - Guidance for Reasonable Methods
- Data Security
  - Data Security Checklist
  - Data Governance Checklist
  - Cloud Computing
  - Identity Authentication Best Practices
  - Data Breach Response Checklist
- FERPA online training
  - FERPA 101 professional training video
  - FERPA 201 (Data Sharing) professional training video
  - FERPA 301 (Postsecondary) professional training video

Contact Information

Privacy Technical Assistance Center

Family Policy Compliance Office

Telephone: (202) 260-3887

Email: FERPA@ed.gov

FAX: (202) 260-9001

Website: www.ed.gov/fpco

Privacy Technical Assistance Center

Telephone: (855) 249-3072

Email: privacyTA@ed.gov

FAX: (855) 249-3073

Website: www.ptac.ed.gov