CERIAS

Privacy: The K-12 Link

M. Dark, C. McPherson[1], J. Troutner[2]
[1]CERIAS, Purdue University, [2]Tipp. School Corporation

- Goals
  - Enable The K-12 Community To:
    - Understand and Differentiate between Privacy and Security
    - Identify threats to privacy
    - Understand relevant privacy laws and regulations (HIPAA, FERPA, CIPA, COPPA)
    - Implement Privacy Preserving Strategies
- Approach
  - Three interactive workshops designed for K-12, with K-12

Module 1

- Privacy Basics
  - Trust, Security & Privacy Defined
  - Privacy Laws
  - Malware & Phishing
  - K-12 Administrative Responsibility
  - Interpreting Privacy Policies

Module 2

- Privacy Best Practices
  - Removing Malware and Select Tools and Services
  - Developing Privacy Policies
  - Encrypting… What, When, Why and How
  - Privacy Preserving Browser Settings
  - Privacy Enhancing Technologies (What, When and Why)

Module 1 End of Module Assessment

Criteria	Question	Score	Relative Weight	Relative Score
	4 = Yes 3 = Being Implemented 2 = Being Discussed 1 = No			
A. Privacy Basics				
25%	1. Does your school corporation separate security and privacy?		0.2	0
	2. Is there anyone that is responsible for privacy related issues in the school corporation?		0.25	0
	3. Does privacy have a line item in the budget?			
	4. Is an annual report on the level of privacy compliance issued to relevai management?			
	5. Are areas containing sensitive information properly secured?			
	6. Is confidential information properly secured?			
	7. Are passwords and accounts being shared?			
	Total Score			
	4 = Yes/Often 3 = Sometimes 2 = Rarely			
B. Malware				
13%	1. Do your computer systems block or prevent banner ads and "pop ups"			
	2. Do your computer systems perform at capacity (not sluggish)?			
	3. Do you have mechanisms to prevent the installation of free and share programs on your systems?			
	4. Are administers, teachers and staff prevented from downloading and installing software?			
	5. Is software downloaded from underground warez sites installed on you computer systems?			
	6. Do your browser settings remain constant and unchanged (e.g. the hon page is never different than the one you set)?			
	7. There are no additional toolbars on your browser?			
	8. You organization has mechanisms in place to ensure that spyware doe not negatively affect privacy.			
	9. Viruses have never negatively impacted your corporation.			
	10. Can you identify the major sources of malware in your corporation?			
	11. Are there any technological solutions in place to mitigate malware or your systems?			
	12. Are your employees aware of the dangers of opening attachments in emails?			
	Total Score			
	4 = Yes 3 = Being Implemented 2 = Being Di			
C. Phishing				
12%	1. Is there any awareness program about phising attempts that might be relevant to your corporation?			
	2. Do you think your employees are able to detect phising attempts?			
	3. Have phishing attacks caused privacy or security problems for your organizations in the past year			
	4. Do you block executables?			
	5. Do you block HTML transmitted through email?			
	6. Are you a subscriber to any of the popular phising scams corporations (ebay, chase, etc)?			
	Total Score			

	4 = Yes 3 = Being Implemented 2 = Being Discussed 1 = No				
D. Responsibility					
25%	1. Do you encourage your staff and students to read the privacy statements on websites before registering on it?		0.05	0	
	2. Do you encourage your staff and students to share their personal information only after reviewing privacy statements?		0.05	0	
	3. Are employees trained to be cognizant of privacy matters?		0.05	0	
	4. Is access to sensitive/confidential information by contractors monitored?		0.05	0	
	5. Do employees receive training on privacy relative to their experience and responsibilities?		0.1	0	
	6. Are employees receiving both positive and negat privacy on their performance evaluations?				
	7. Are administrators given additional privacy spec				
	8. Is there a regular privacy awareness program in j				
	9. Are audit logs or other reporting mechanisms in containing sensitive information?				
	10. Are violations to privacy tracked?				
	11. Are procedures in place for the proper disposal information?				
	12. Are unsecured and temporary accounts restricte information and disabled in a timely fashion?				
	13. Have employees been trained on proper passwo				
	14. Are permissions being properly set (only those information have access to it)?				
	15. Are users of all network resources required to c password?				
	16. Are Access Control Lists maintained on a regul				
	Total Sc				
	4 = Yes 3 = Being Implemented				
E. Privacy Policies					
	1. Do you have a website?				
	If the answer to Q1 is yes continue below… If t				
	2. Does your website target group include children				
	3. Does your website collect email addresses?				
	4. Does your website collect personal identifying ir email address (name, address, telephone number, cr social security number)?				
	5. Is there a privacy policy for your website?				
	If the answer to Q5 is yes continue below… If the answer it no, go to Q16				
	6. Does the Privacy Policy state anything about what specific personal information is collected?		0.1	0	
	7. Does the Privacy Policy state how the website may use personal information it collects for internal purposes?		0.05	0	
	8. Does the Privacy Policy state anything about the website's use of personal information collected to send communications to visitors?		0.05	0	
	9. Does the Privacy Policy state anything about the website's right to disclose personal information to third parties?		0.05	0	
25%	10. Does the Privacy Policy say whether the website allows users to review, modify and delete some of the personal information collected about them?		0.05	0	
	11. Does the Privacy Policy say what measures the website takes to provide security?		0.05	0	
	12. Does the Privacy Policy say what measures are taken to provide security for personal information during the transmission from the consumer to the website?		0.05	0	
	13. Does the Privacy Policy say what measures are taken to secure personal information after it has been collected?		0.1	0	
	14. Does the Privacy Policy say whether the website places cookies or not?		0.05	0	
	15. Does the Privacy Policy say whether third parties may place cookies or collect personal information on the website?		0.05	0	
	16. Does your corporation have any plans to develop a privacy policy for your website?		0.6		
	17. Do you have a document that describes the type of information collected in your corporation?		0.2		
	18. Do you have a policy that documents the privacy practices of your corporation?		0.3		
	19. Do information providers have any options when disclosing information?		0.2		
	20. Do you have a policy that states the right to disclose personal information to third parties?		0.2		
	21. Do you have a policy that states how sensitive information collected is stored and secured?		0.1		
	Total Score				0

Law	Law Type	Vulnerability / Threat	Strategic Emphasis	Practices		
				Policy	Technology	Administrative
FERPA Family Education Rights and Privacy Act - 1974	*Privacy*	*Twin Vulnerabilities: unauthorized **access** or **disclosure**.* **Access vulnerabilities:** • *Confidential data, transmitted over Internet in unencrypted format, is intercepted* • *External intruder hacks in* • *Internal scofflaw steals password or hacks in* **Disclosure vulnerabilities:** • *Authorized users fail to follow rules* • *Staff inadvertently reveals protected data in hardcopy format*	• *Secure the borders:* stop protected information from **getting out** - and into the wrong hands with regularly updated and maintained firewall, wireless access protections, etc. • *Improve internal network security:* Create and enforce authentication and authorization policies and procedures for role-based access to data. • *Encryption*: protected data should never be stored or released in an unprotected format. Hardcopy should be in locked cabinets or only given out in sealed envelopes; electronic material should be stored and sent in encrypted format. • *Many players - one playbook*: technology won't protect you if authorized staffs don't know the rules about releasing data or leaving logged-in machines unattended. Train and remind everyone about appropriate practices.	• Privacy Policies	• Encryption for storage and transmission of data • Network security • Physical security	• Educational & Training Awareness Programs
CIPA Children's Internet Protection Act - 2000	*Security*	• *Email: Spam* • *Web: pornography, violent or hate sites* • *Other inappropriate content originating outside - or inside - the network*	• *All along the watchtower:* Reduce the likelihood that inappropriate information will **enter** your network with appropriately configured filters. In Particular: review spam filtering methodology regularly. However, the law only requires meaningful effort, not perfection, since there is no foolproof technological solution. • *The human element:* Be public about the inevitability that some inappropriate material will slip through and train students (and staff) how to deal with it. Make sure everyone knows the district's policies and penalties concerning harassment, use of school resources for inappropriate purposes, etc.	• Usage Policies	• Email filtering • Internet filtering	• Educational & Training Awareness Programs • Student Online Supervision
HIPAA Health Insurance Portability and Accountability Act - 1996	*Privacy*	• *School nurse or athletic department needs health information. Local public health department may request assistance documenting immunization,*	• *Get it in writing:* A school district can NOT legally be given medical information about a particular person without first receiving HIPAA-required permission. Make sure that parents and staff have given explicit, written permission for you to receive medical data. Once in the district, however, medical info of students falls under FERPA rules.	• Privacy Policies • Usage Policies	• Encryption for storage and transmission of data • Network security • Physical security	• Educational & Training Awareness Programs
COPA Child Online	*Privacy*	• *Potentially impacts district web sites or discussion forums that*	• *Freedom of Speech:* Free speech argument tips a Supreme Court injunction 5-4 (June 2004) against	• Privacy Policies	• Internet filtering	• Educational & Training

Modified from Cyber Security Project Materials by Steven Miller

Module 3

- Future Trends
  - Digital Identity Management
  - Privacy & Security: Information Privacy Policies
  - Privacy in Reusable Digital Devices
  - Purpose Based Access Control

PURDUE UNIVERSITY · PURDUE HOMELAND SECURITY INSTITUTE · CERIAS · REGENSTRIEF CENTER FOR HEALTHCARE ENGINEERING · Discovery Park e-Enterprise Center