Safe computing

Introduction

CSCI E 45b: The Cyber World – part B

Introduction: learning goals

- Taking a pragmatic view into information security

  Protecting an enterprise

  Protecting you (and others around you)
- Looking at known information security frameworks to see if they can help, even beyond their original intended use

Topics

SAFE AND SECURE COMPUTING

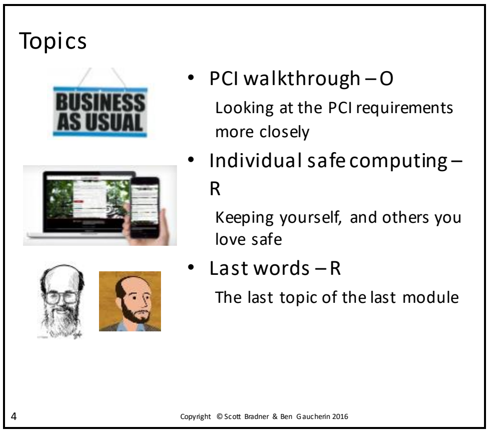
PCI Security Standards Council

- Enterprise safe computing – R

  What does it mean to keep an enterprise safe?
- Enterprise security standards – R

  Information security standards and frameworks
- PCI Intro – R

  Introduction to the PCI DSS standard



Topics

- PCI walkthrough – O

  Looking at the PCI requirements more closely
- Individual safe computing – R

  Keeping yourself, and others you love safe
- Last words – R

  The last topic of the last module

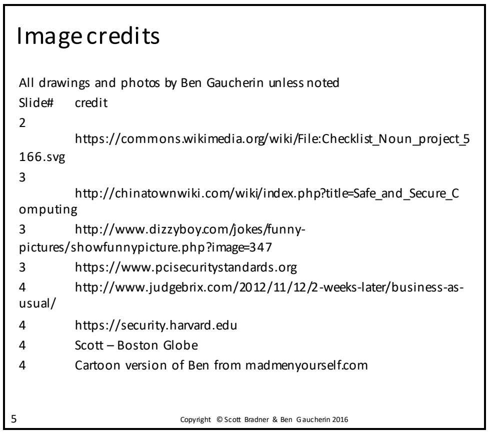
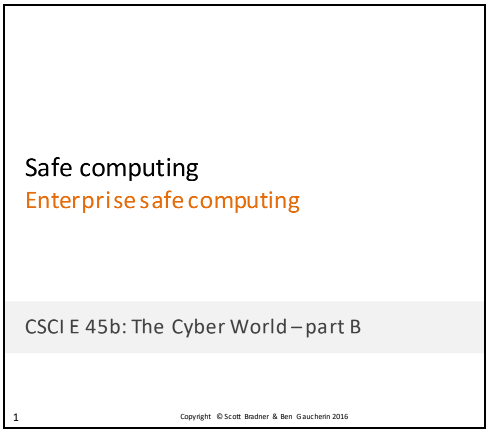


Image credits

All drawings and photos by Ben Gaucherin unless noted

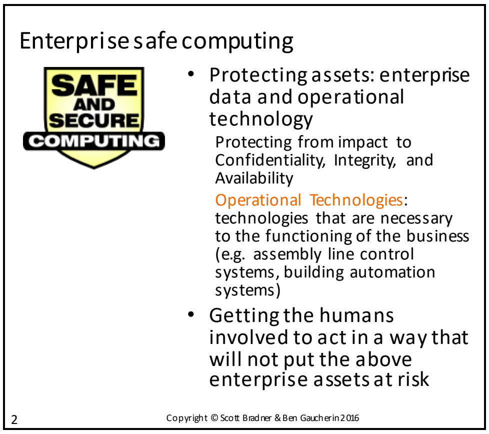
Slide#	credit
2	https://commons.wikimedia.org/wiki/File:Checklist_Noun_project_5166.svg
3	http://chinatownwiki.com/wiki/index.php?title=Safe_and_Secure_Computing
3	http://www.dizzyboy.com/jokes/funny-pictures/showfunnypicture.php?image=347
3	https://www.pcisecuritystandards.org
4	http://www.judgebrix.com/2012/11/12/2-weeks-later/business-as-usual/
4	https://security.harvard.edu
4	Scott – Boston Globe
4	Cartoon version of Ben from madmenyourself.com



Safe computing

Enterprise safe computing

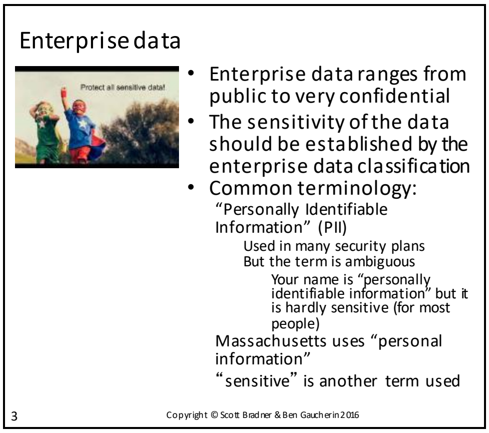
CSCI E 45b: The Cyber World – part B



SAFE AND SECURE COMPUTING

Enterprise safe computing

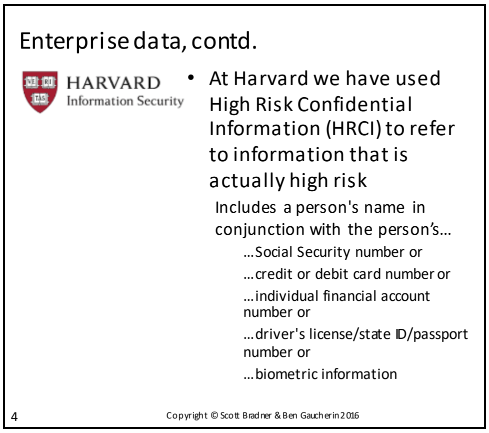
- Protecting assets: enterprise data and operational technology
  - Protecting from impact to Confidentiality, Integrity, and Availability
  - Operational Technologies: technologies that are necessary to the functioning of the business (e.g. assembly line control systems, building automation systems)
- Getting the humans involved to act in a way that will not put the above enterprise assets at risk



Protect all sensitive data!

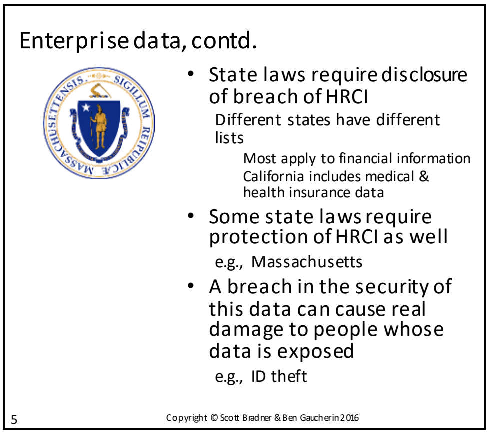
Enterprise data

- Enterprise data ranges from public to very confidential
- The sensitivity of the data should be established by the enterprise data classification
- Common terminology:
  - "Personally Identifiable Information" (PII)
    - Used in many security plans
    - But the term is ambiguous
      - Your name is "personally identifiable information" but it is hardly sensitive (for most people)
  - Massachusetts uses "personal information"
  - "sensitive" is another term used



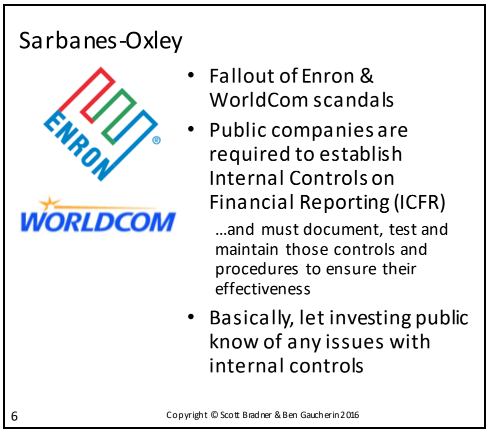
Enterprise data, contd.

- At Harvard we have used High Risk Confidential Information (HRCI) to refer to information that is actually high risk
  - Includes a person's name in conjunction with the person's…
    - …Social Security number or
    - …credit or debit card number or
    - …individual financial account number or
    - …driver's license/state ID/passport number or
    - …biometric information



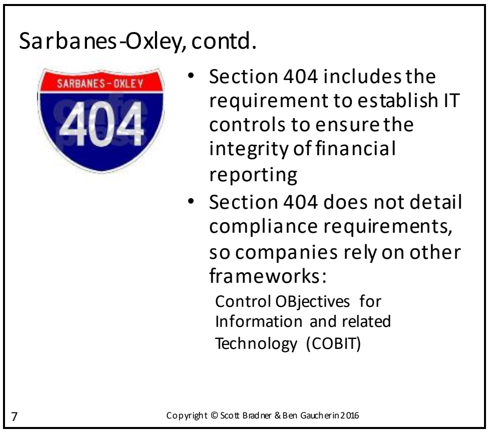
Enterprise data, contd.

- State laws require disclosure of breach of HRCI
  - Different states have different lists
    - Most apply to financial information
    - California includes medical & health insurance data
- Some state laws require protection of HRCI as well
  - e.g., Massachusetts
- A breach in the security of this data can cause real damage to people whose data is exposed
  - e.g., ID theft



Sarbanes-Oxley

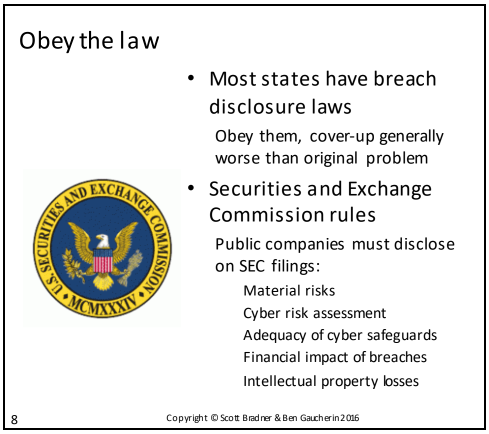
- Fallout of Enron & WorldCom scandals
- Public companies are required to establish Internal Controls on Financial Reporting (ICFR)
  - …and must document, test and maintain those controls and procedures to ensure their effectiveness
- Basically, let investing public know of any issues with internal controls



Sarbanes-Oxley, contd.

SARBANES - OXLEY
404

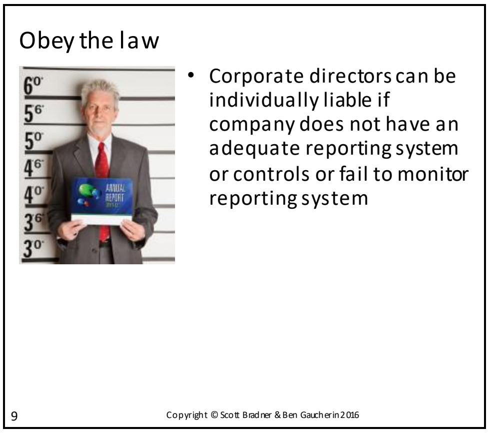
- Section 404 includes the requirement to establish IT controls to ensure the integrity of financial reporting
- Section 404 does not detail compliance requirements, so companies rely on other frameworks:
  - Control OBjectives for Information and related Technology (COBIT)



Obey the law

U.S. SECURITIES AND EXCHANGE COMMISSION
MCMXXXIV

- Most states have breach disclosure laws
  - Obey them, cover-up generally worse than original problem
- Securities and Exchange Commission rules
  - Public companies must disclose on SEC filings:
    - Material risks
    - Cyber risk assessment
    - Adequacy of cyber safeguards
    - Financial impact of breaches
    - Intellectual property losses



Obey the law

ANNUAL REPORT

- Corporate directors can be individually liable if company does not have an adequate reporting system or controls or fail to monitor reporting system

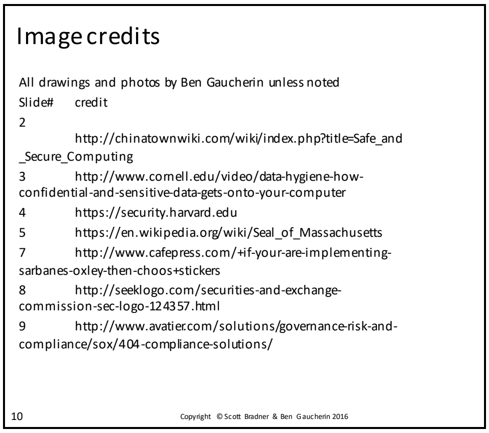
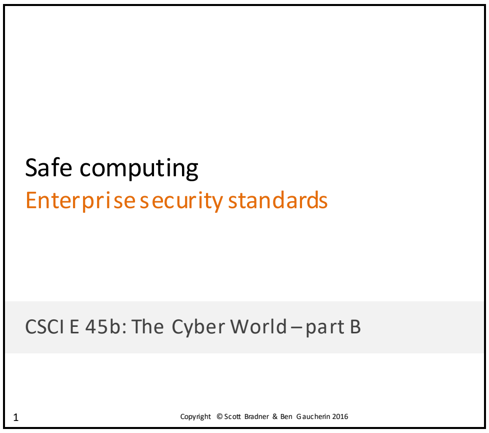


Image credits

All drawings and photos by Ben Gaucherin unless noted

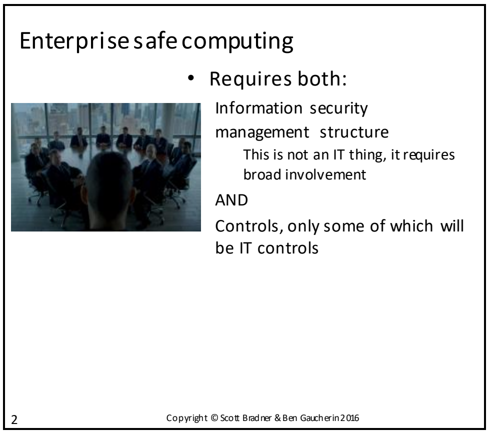
Slide#	credit
2	http://chinatownwiki.com/wiki/index.php?title=Safe_and_Secure_Computing
3	http://www.cornell.edu/video/data-hygiene-how-confidential-and-sensitive-data-gets-onto-your-computer
4	https://security.harvard.edu
5	https://en.wikipedia.org/wiki/Seal_of_Massachusetts
7	http://www.cafepress.com/+if-your-are-implementing-sarbanes-oxley-then-choos+stickers
8	http://seeklogo.com/securities-and-exchange-commission-sec-logo-124357.html
9	http://www.avatier.com/solutions/governance-risk-and-compliance/sox/404-compliance-solutions/



Safe computing

Enterprise security standards

CSCI E 45b: The Cyber World – part B



Enterprise safe computing

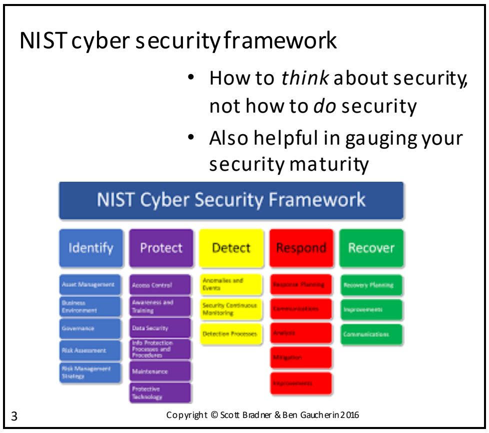
- Requires both:

Information security management structure

This is not an IT thing, it requires broad involvement

AND

Controls, only some of which will be IT controls



NIST cyber security framework

- How to *think* about security, not how to *do* security
- Also helpful in gauging your security maturity

NIST Cyber Security Framework

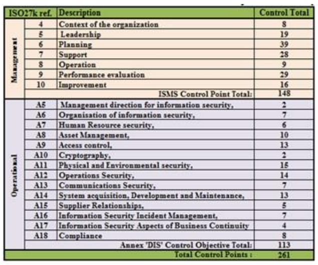
Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

ISO/IEC 27001

- BS7799 - Corporate security standard donated by Shell to a UK government initiative in the early 1990s
- Became ISO/IEC 17799, then renumbered to be ISO/IEC 27002
- But, ISO/IEC 27002 is merely a set of recommendations
- This led to the creation of ISO/IEC 27001 to allow for audit and certification

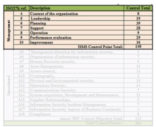
Overview of ISO/IEC 27001:2013

- Defines the requirements for an Information Security Management System (ISMS)



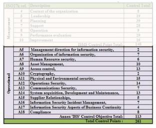
ISO27k ref.		Description	Control Total
Management	4	Context of the organization	8
	5	Leadership	19
	6	Planning	39
	7	Support	28
	8	Operation	9
	9	Performance evaluation	29
	10	Improvement	16
		ISMS Control Point Total:	148
Operational	A5	Management direction for information security,	2
	A6	Organisation of information security,	7
	A7	Human Resource security,	6
	A8	Asset Management,	10
	A9	Access control,	13
	A10	Cryptography,	2
	A11	Physical and Environmental security,	15
	A12	Operations Security,	14
	A13	Communications Security,	7
	A14	System acquisition, Development and Maintenance,	13
	A15	Supplier Relationships,	5
	A16	Information Security Incident Management,	7
	A17	Information Security Aspects of Business Continuity	4
	A18	Compliance	8
		Annex 'DIS' Control Objective Total:	113
		Total Control Points :	261

The mandatory controls - Clauses 4-10



4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operations
9. Performance evaluation
10. Improvements

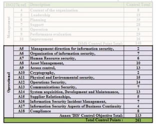
The discretionary controls - Annex A



ISO27k ref.		Description	Control Total
Management	4	Context of the organization	8
	5	Leadership	19
	6	Planning	39
	7	Support	28
	8	Operation	9
	9	Performance evaluation	29
	10	Improvement	16
		ISMS Control Point Total:	148
Operational	A5	Management direction for information security,	2
	A6	Organisation of information security,	7
	A7	Human Resource security,	6
	A8	Asset Management,	10
	A9	Access control,	13
	A10	Cryptography,	2
	A11	Physical and Environmental security,	15
	A12	Operations Security,	14
	A13	Communications Security,	7
	A14	System acquisition, Development and Maintenance,	13
	A15	Supplier Relationships,	5
	A16	Information Security Incident Management,	7
	A17	Information Security Aspects of Business Continuity	4
	A18	Compliance	8
		Annex 'DIS' Control Objective Total:	113
		Total Control Points :	261

- A.5 Information security policies
- A.6 Organization of information security
- A.7 Human resource security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operations security

The discretionary controls - Annex A, contd.



ISO27k ref.		Description	Control Total
Management	4	Context of the organization	8
	5	Leadership	19
	6	Planning	39
	7	Support	28
	8	Operation	9
	9	Performance evaluation	29
	10	Improvement	16
		ISMS Control Point Total:	148
Operational	A5	Management direction for information security,	2
	A6	Organisation of information security,	7
	A7	Human Resource security,	6
	A8	Asset Management,	10
	A9	Access control,	13
	A10	Cryptography,	2
	A11	Physical and Environmental security,	15
	A12	Operations Security,	14
	A13	Communications Security,	7
	A14	System acquisition, Development and Maintenance,	13
	A15	Supplier Relationships,	5
	A16	Information Security Incident Management,	7
	A17	Information Security Aspects of Business Continuity	4
	A18	Compliance	8
		Annex 'DIS' Control Objective Total:	113
		Total Control Points :	261

- A.13 Communications security
- A.14 System acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance

FISMA

- Federal Information Systems Management Act (FISMA)
- 2002 law requiring federal agencies to meet baseline standards in information security
- Extends to organizations/institutions working with the federal government

  e.g., Universities when doing government funded research

FISMA, contd.

- NIST Special Publication 800-53 defines the controls and compliance requirements

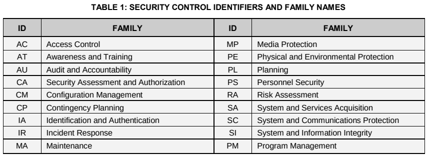


TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

FISMA, contd.

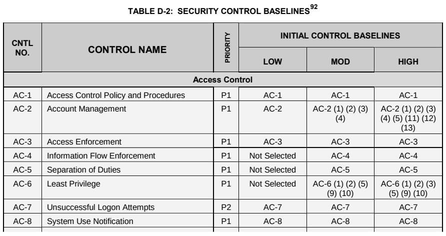
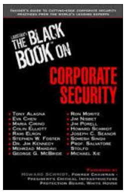


TABLE D-2: SECURITY CONTROL BASELINES[92]

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
	Access Control				
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8

Extract form the Security Control Baselines table in NIST 800-53

But will your enterprise be safe?



- Full compliance with standards will make your data safer
  - Make it harder for something bad to happen
  - Limit impact if something bad happens
  - Improve your ability to respond appropriately to a bad event
- But will not make you safe (in the absolute sense)

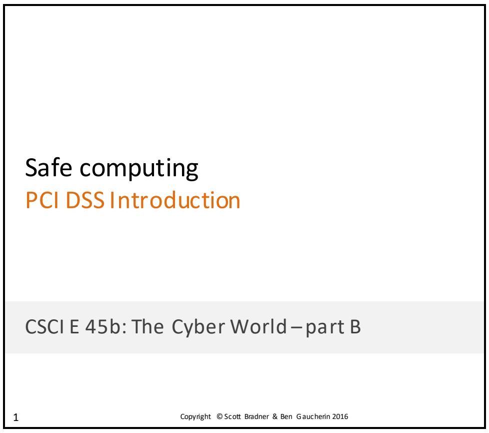
But will your enterprise be safe?

- Not a protection against stupidity or bad decisions
  See ChoicePoint type problems
- Still requires thinking!

Image credits

All drawings and photos by Ben Gaucherin unless noted

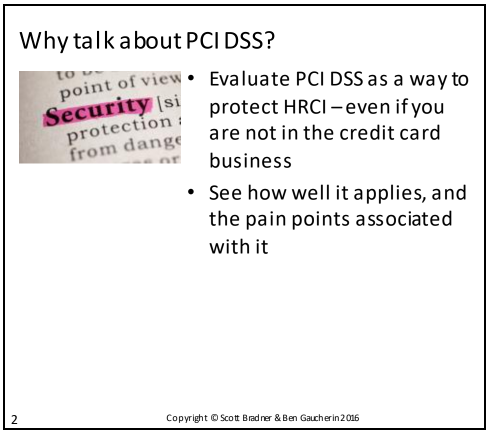
Slide#	credit
2	http://www.patch-music.com/blog/2015/9/30/mr-robot
3	http://www.tieuluu.com/blog/2015/06/nist-cyber-security-framework.html
4	http://www.quotium.com/resources/application-security-iso27001-compliance-seeker-can-help/
5	http://www.bluekaizen.org/isoiec-270012013-part2/
5-8	http://www.itworldcanada.com/blog/the-new-isms-isoiec-270012013-expert-insight/84379
9	https://www.datapipe.com/security_compliance/compliance/
10, 11	Extracts from NITS SP 800-53
12	http://www.barnesandnoble.com/w/larstans-the-black-book-on-corporate-security-larstan-publishing/1101348365
13	http://www.dizzyboy.com/jokes/funny-pictures/showfunnypicture.php?image=347



Safe computing

PCI DSS Introduction

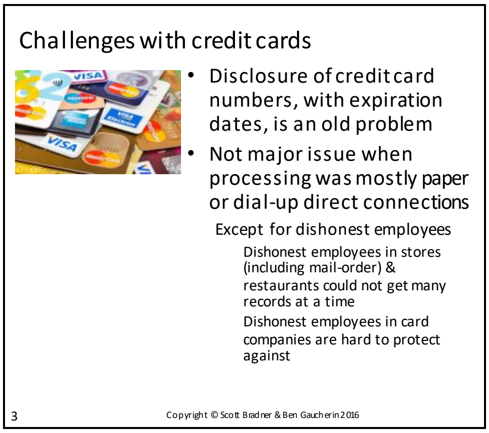
CSCI E 45b: The Cyber World – part B



Why talk about PCI DSS?

point of view
Security [si
protection
from dange

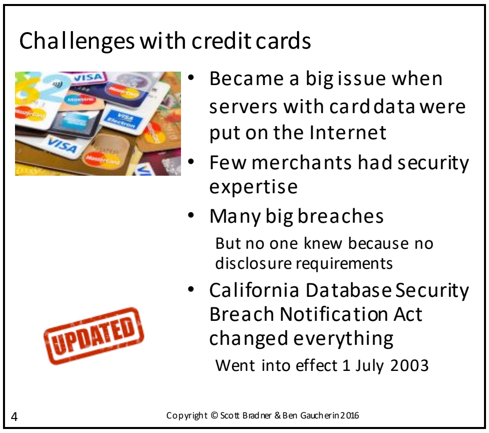
- Evaluate PCI DSS as a way to protect HRCI – even if you are not in the credit card business
- See how well it applies, and the pain points associated with it



Challenges with credit cards

VISA
VISA
MasterCard

- Disclosure of credit card numbers, with expiration dates, is an old problem
- Not major issue when processing was mostly paper or dial-up direct connections
  - Except for dishonest employees
    - Dishonest employees in stores (including mail-order) & restaurants could not get many records at a time
    - Dishonest employees in card companies are hard to protect against



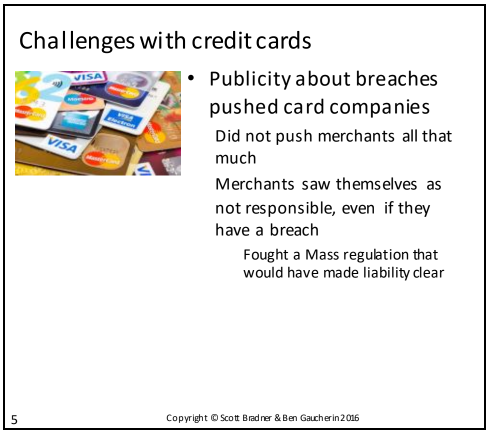
Challenges with credit cards

- Became a big issue when servers with card data were put on the Internet
- Few merchants had security expertise
- Many big breaches

  But no one knew because no disclosure requirements
- California Database Security Breach Notification Act changed everything

  Went into effect 1 July 2003

4 Copyright © Scott Bradner & Ben Gaucherin 2016



Challenges with credit cards

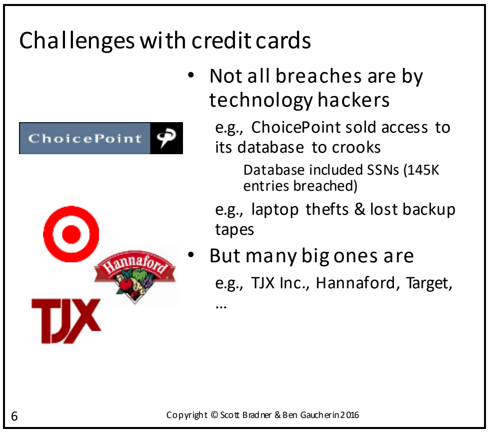
- Publicity about breaches pushed card companies

  Did not push merchants all that much

  Merchants saw themselves as not responsible, even if they have a breach

  Fought a Mass regulation that would have made liability clear

5 Copyright © Scott Bradner & Ben Gaucherin 2016



Challenges with credit cards

- Not all breaches are by technology hackers

  e.g., ChoicePoint sold access to its database to crooks

  Database included SSNs (145K entries breached)

  e.g., laptop thefts & lost backup tapes
- But many big ones are

  e.g., TJX Inc., Hannaford, Target, …

6 Copyright © Scott Bradner & Ben Gaucherin 2016

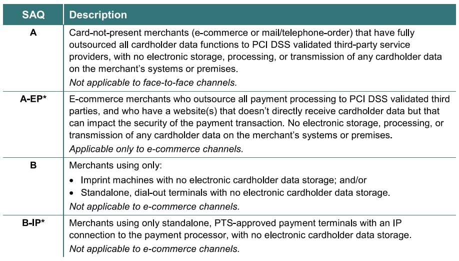
PCI DSS

- Payment Card Industry (PCI) Data Security Standard (DSS)
- Defined and enforced by an industry group
  - Not a law, but contracts amongst participants in the "payment chain" ensure everyone does the right thing
  - Failure to comply may mean inability to process credit cards
- Scope: All technologies and humans involved in the payment chain

PCI's alphabet soup

- SAQ – Self-Assessment Questionnaire
  - Questionnaire to assess the requirements/controls that apply
- AOC- Attestation Of Compliance
  - What you can obtain if you meet the requirements tested by an SAQ
- QSA - Qualified Security Assessor
  - Individual registered and trained to do formal assessments

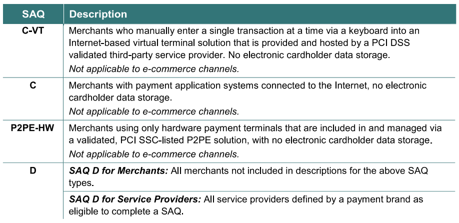
Different SAQs



SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Not applicable to face-to-face channels.*
A-EP*	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. *Applicable only to e-commerce channels.*
B	Merchants using only: • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
B-IP*	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*

From "Understanding the SAQs for PCI DSS version 3

Different SAQs, contd.



SAQ	Description
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. *Not applicable to e-commerce channels.*
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. *Not applicable to e-commerce channels.*
P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. *Not applicable to e-commerce channels.*
D	***SAQ D for Merchants:*** All merchants not included in descriptions for the above SAQ types.
	SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete a SAQ.

From “Understanding the SAQs for PCI DSS version 3

Image credits

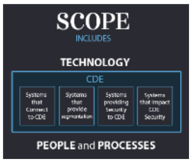
All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
2	https://www.pcisecuritystandards.org/pci_security/glossary
3-5	http://earlyretirementahead.com/2015/05/dangers-of-credit-card-rewards/
6	Target, ChoicePoint, Hannaford, TJX logos
7	https://www.pcisecuritystandards.org
8	http://www.experian.com/blogs/insights/2016/02/compliance-definitions/
9-10	Extracts from “Understanding the SAQs for PCI DSS version 3” from pcisecuritystandards.org

Safe computing
PCI walkthrough

CSCI E 45b: The Cyber World – part B

PCI DSS scope

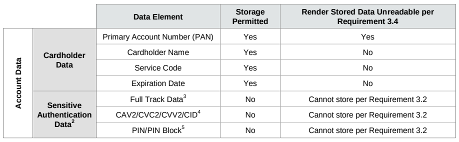

SCOPE
INCLUDES
TECHNOLOGY
CDE
Systems that Connect to CDE
Systems that provide segmentation
Systems providing Security to CDE
Systems that impact CDE Security
PEOPLE and PROCESSES

The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. "System components" include network devices, servers, computing devices, and applications.

Make it Business As Usual (BAU)

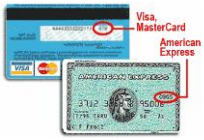
To ensure security controls continue to be properly implemented, PCI DSS should be implemented into business-as-usual (BAU) activities as part of an entity's overall security strategy. This enables an entity to monitor the effectiveness of their security controls on an ongoing basis, and maintain their PCI DSS compliant environment in between PCI DSS assessments.

Don't store everything



		Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[2]	Full Track Data[3]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID[4]	No	Cannot store per Requirement 3.2
		PIN/PIN Block[5]	No	Cannot store per Requirement 3.2

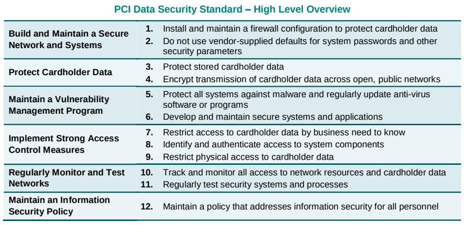
- CVV2 is visible on the card but is not on the magnetic strip



PCI DSS overview

- 12 requirements, specific controls for each

  Technical controls are not always the right solution



PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

From "Requirements and security assessment procedures version 3.1"

Requirement 1

- Install and maintain a firewall configuration to protect cardholder data

  Compartmentalize the network

  No access from the public Internet

  Establish standards and formal processes

  Have policies and procedures to ensure the above is done

Requirement 2

CIRT.net suspicion breeds

Home

Default Passwords

Search

374 vendors, 1715 passwords

360 Systems	3COM	Acc
ACCTON	Acer	Acti
Adaptec	ADC Kentrox	AdCi
Adtech	AdTran	Adv
AirLink Plus	Aironet	Airw
Aladdin	Alcatel	Alle
Allnet	Allot	Alte
Ambit	AMI	Amp
Amptron	Apache	Apac
APC	Apple Computer	Arro
Aruba	Asante	Asce
AST	Asus	AT&

Online database of default username/passwords

- Do not use vendor-supplied defaults for system passwords and other security parameters
  - No vendor-supplied defaults accounts
  - Establish standards and formal processes for system hardening
  - Ensure all known vulnerabilities are addressed
  - Encrypt all non-console administrative access

Requirement 2, contd.

CIRT.net suspicion breeds

Home

Default Passwords

Search

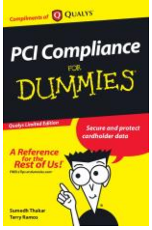
374 vendors, 1715 passwords

360 Systems	3COM	Acc
ACCTON	Acer	Acti
Adaptec	ADC Kentrox	AdCi
Adtech	AdTran	Adv
AirLink Plus	Aironet	Airw
Aladdin	Alcatel	Alle
Allnet	Allot	Alte
Ambit	AMI	Amp
Amptron	Apache	Apac
APC	Apple Computer	Arro
Aruba	Asante	Asce
AST	Asus	AT&

Online database of default username/passwords

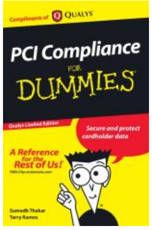
- Maintain an inventory of all system components
- Have policies and procedures to ensure the above is done

Requirement 3


Compliments of QUALYS
PCI Compliance FOR DUMMIES
Qualys Limited Edition
Secure and protect cardholder data
A Reference for the Rest of Us!
Sumedh Thakar
Terry Ramos

- Protect stored cardholder data
  - Only store what you are allowed to store, in the way you are expected to store it, and only for the time you need it
  - Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes

Requirement 3, contd.



Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse

Have policies and procedures to ensure the above is done

Requirement 4

- Encrypt transmission of cardholder data across open, public networks

Use strong cryptography and security protocols to protect data in transit

Never send unprotected PANs by end- user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).

Have policies and procedures to ensure the above is done

Requirement 5

- Protect all systems against malware and regularly update anti-virus software or programs

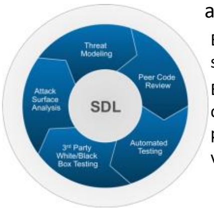
Deploy anti-virus software on all systems

Ensure that all anti-virus mechanisms are maintained

Ensure that anti-virus mechanisms are actively running and cannot be disabled

Have policies and procedures to ensure the above is done

Requirement 6



- Develop and maintain secure systems and applications

Establish a process to identify security vulnerabilities

Ensure that all system components and software are patched to protect from known vulnerabilities

Prioritize to address high impact vulnerabilities first

Develop software securely

Follow change control protocols

Requirement 6, contd.

Address new threats and vulnerabilities on an ongoing basis

Have policies and procedures to ensure the above is done

Requirement 7

NEED TO KNOW

- Restrict access to cardholder data by business need to know

Limit access to only those who need access

Establish access control system with "deny all" as default

Have policies and procedures to ensure the above is done

Requirement 8

TARGET

- Identify and authenticate access to system components

Ensure proper user identification management for non- consumer users and administrators

Incorporate two-factor authentication for remote network access originating from outside the network by personnel and all third parties

Document and communicate authentication policies and procedures to all users

Requirement 8, contd.

Do not use group, shared, or generic IDs, passwords, or other authentication methods

Have policies and procedures to ensure the above is done

HARVARDKEY

Requirement 9

- Restrict physical access to cardholder data

The data center has to be physically and operationally protected

Develop procedures to easily distinguish between onsite personnel and visitors

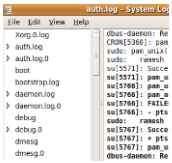
Physically secure and control the distribution, storage, and disposal of all media.

Requirement 9, contd.

Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.

Have policies and procedures to ensure the above is done

Requirement 10



```
dbus-daemon: Re
CRON[5360]: pam
sudo: pam_unix(
sudo:   ramesh
su[5571]: Succe
su[5571]: pam_u
su[5766]: pam_u
su[5766]: pam_a
su[5766]: FAILE
su[5766]: - pts
sudo:   ramesh
su[5767]: Succe
su[5767]: + pts
su[5767]: pam_u
dbus-daemon: Re
```

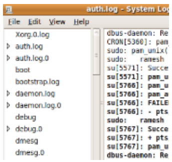
- Track and monitor all access to network resources and cardholder data

Implement audit trails (logs) to link all access to system components to each individual user and send them to a protected server

Secure the logs so they cannot be altered

Review logs and security events for all system components to identify anomalies or suspicious activity

Requirement 10, contd.



```
dbus-daemon: Re
CRON[5360]: pam
sudo: pam_unix(
sudo:   ramesh
su[5571]: Succe
su[5571]: pam_u
su[5766]: pam_u
su[5766]: pam_a
su[5766]: FAILE
su[5766]: - pts
sudo:   ramesh
su[5767]: Succe
su[5767]: + pts
su[5767]: pam_u
dbus-daemon: Re
```

Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis

Have policies and procedures to ensure the above is done

Requirement 11

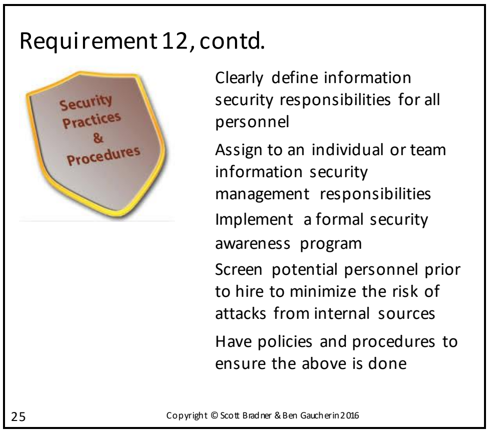
- Regularly test security systems and processes
  - Implement processes to test for the presence of wireless access points
  - Run internal and external network vulnerability scans at least quarterly and after any significant change in the network
    - External scan needs to be run by approved third party
  - Implement a methodology for penetration testing

Requirement 11

- Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network
- Deploy a change-detection mechanism to alert personnel to unauthorized modification
- Have policies and procedures to ensure the above is done

Requirement 12

- Maintain a policy that addresses information security for all personnel
  - Establish, publish, maintain, and disseminate a security policy
  - Implement a risk-assessment process
  - Develop usage policies for critical technologies and define proper use of these technologies



Requirement 12, contd.

Security
Practices
&
Procedures

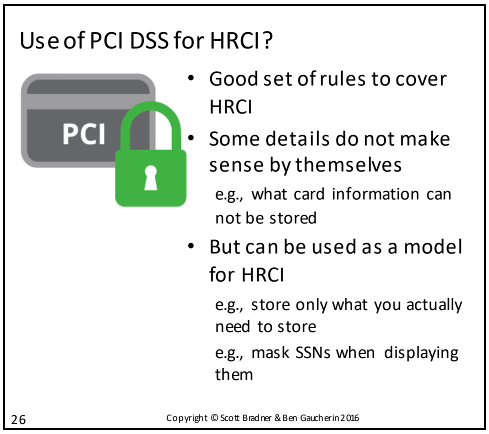
Clearly define information security responsibilities for all personnel

Assign to an individual or team information security management responsibilities

Implement a formal security awareness program

Screen potential personnel prior to hire to minimize the risk of attacks from internal sources

Have policies and procedures to ensure the above is done



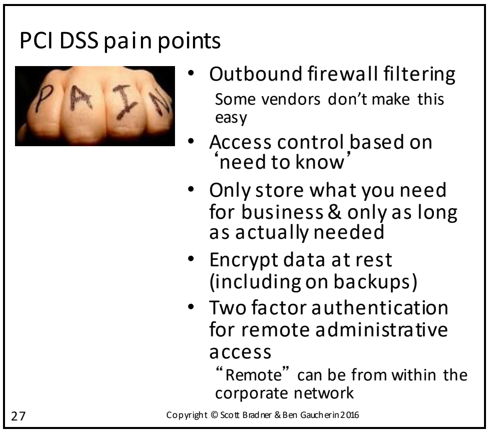
Use of PCI DSS for HRCI?

- Good set of rules to cover HRCI
- Some details do not make sense by themselves

  e.g., what card information can not be stored
- But can be used as a model for HRCI

  e.g., store only what you actually need to store

  e.g., mask SSNs when displaying them



PCI DSS pain points

- Outbound firewall filtering

  Some vendors don't make this easy
- Access control based on 'need to know'
- Only store what you need for business & only as long as actually needed
- Encrypt data at rest (including on backups)
- Two factor authentication for remote administrative access

  "Remote" can be from within the corporate network

PCI DSS pain points

- No developer access to production systems
- Periodic password change

28 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
2	http://www.carsoninc.com/blog/pci-compliance-2-scope
3	http://www.judgebrix.com/2012/11/12/2-weeks-later/business-as-usual/
4	https://www.cvvnumber.com/
5	Extract from "Requirements and security assessment procedures version 3.1" from pcisecuritystandards.org
6	https://www.firemon.com/advancing-firewall-necessary-evils-10-tuple/
7, 8	https://cirt.net/passwords
9, 10	http://www.slideshare.net/Larryz/pci-compliance-for-dummies-48493322
11	http://cpress.org/leftnews/weak-encryption-wont-defeat-terrorists-2013-but-it-will-enable-hackers-guardian
12	http://www.file-extensions.org/article/top-antivirus-software

29 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits, contd.

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
13, 14	https://www.okta.com/a-secure-reliable-service-you-can-trust/
15	http://www.slicktext.com/blog/2015/01/5-things-you-need-to-know-when-using-our-text-message-marketing-service/
16	Target logo
17	HarvardKey logo
18	http://onthetech.com/how-to-build-physical-security-into-a-data-center/
19	http://www.coindesk.com/point-of-sale-giant-ingenico-rolls-out-worldwide-bitcoin-payments/
20, 21	http://www.thegeekstuff.com/2009/11/ubuntu-tips-how-to-view-system-log-files-in-gui/
22, 23	http://docs.kali.org/installation/kali-linux-hard-disk-install
24, 25	https://www.eizyherbal.com/security-policy/
26	https://sucuri.net/website-firewall/pci-compliance
27, 28	http://www.corechiropractic.net/do-you-have-a-high-pain-tolerance/

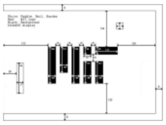
30 Copyright © Scott Bradner & Ben Gaucherin 2016

Safe computing

Safe computing for individuals

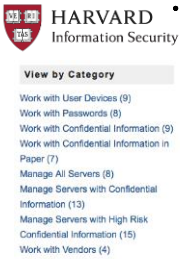
CSCI E 45b: The Cyber World – part B

MIT's Safe Computing Tips



- Patch, patch, PATCH!
- Install protective software.
- Chose strong passwords.
- Backup, Backup, BACKUP!
- Control access to your machine.
- Use email and Internet safely.
- Use secure connections.
- Protect sensitive data.
- Use desktop firewalls.
- Most importantly, stay informed.

Harvard Requirements and 'How To's



HARVARD Information Security

View by Category

Work with User Devices (9)
Work with Passwords (8)
Work with Confidential Information (9)
Work with Confidential Information in Paper (7)
Manage All Servers (8)
Manage Servers with Confidential Information (13)
Manage Servers with High Risk Confidential Information (15)
Work with Vendors (4)

- Let's look at select Requirements and supporting How-To's from Harvard's security policy
  - All users
  - User devices

Harvard Requirements and 'How To's, contd.

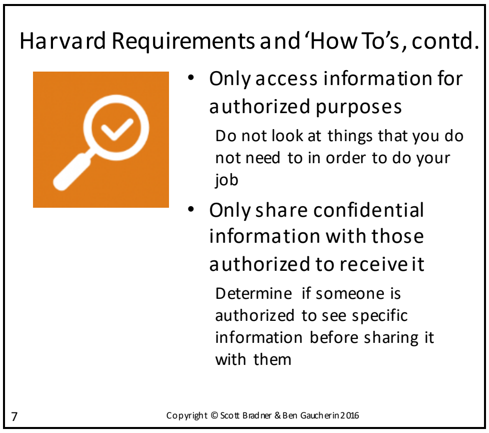
- How to avoid sharing passwords
  - Use shared files (Dropbox, Google docs, etc.)
  - Use delegation in email
- Protecting passwords
  - If written down, treat as HRCI
  - Use a password manager

Password manager

- Application to store and fill usernames & passwords in web pages
  - can also store & auto fill other info
    - e.g., addresses, credit card, etc.
- One master password used to enable application
- Disabled on machine sleep or on timeout
- Can sync across devices
- Use a different password for every web site
  - Ideally long random password

Harvard Requirements and 'How To's, contd.

- Use complex passwords
  - How to select a strong and memorable password
  - Use a password manager and different long random passwords for each system
  - Short (e.g., 4-digit) PIN ok if device auto-wipes after small number of bad guesses
- Change passwords if compromised
  - How to change passwords in various systems

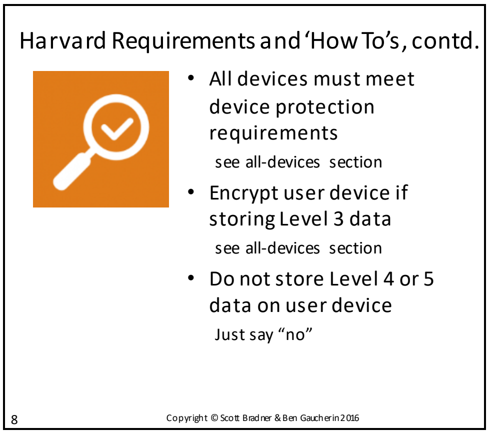


Harvard Requirements and 'How To's, contd.

- Only access information for authorized purposes
  - Do not look at things that you do not need to in order to do your job
- Only share confidential information with those authorized to receive it
  - Determine if someone is authorized to see specific information before sharing it with them

7

Copyright © Scott Bradner & Ben Gaucherin 2016

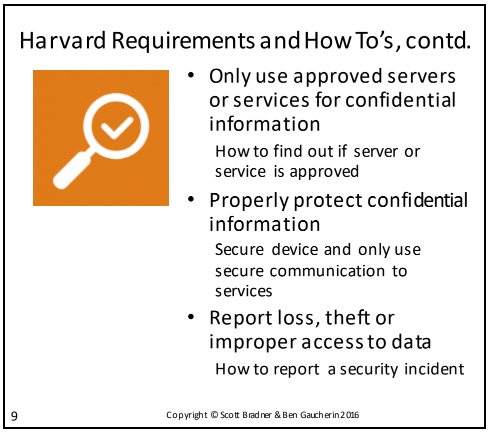


Harvard Requirements and 'How To's, contd.

- All devices must meet device protection requirements
  - see all-devices section
- Encrypt user device if storing Level 3 data
  - see all-devices section
- Do not store Level 4 or 5 data on user device
  - Just say "no"

8

Copyright © Scott Bradner & Ben Gaucherin 2016



Harvard Requirements and How To's, contd.

- Only use approved servers or services for confidential information
  - How to find out if server or service is approved
- Properly protect confidential information
  - Secure device and only use secure communication to services
- Report loss, theft or improper access to data
  - How to report a security incident

9

Copyright © Scott Bradner & Ben Gaucherin 2016

Harvard Requirements and How To's, contd.

- Agree to confidentiality statement
  - How to execute the confidentiality statement
- Handling of credit cards must be approved
  - Who to ask for approval

Harvard Requirements and How To's, contd.

- Configure device for secure operation
  - Smartphones & tablets
    - Use PIN, enable encryption (if not automatic on PIN), auto wipe on small number of bad guesses (or use complex password), enable timeout, enable activation lock (if available)
  - Desktops & laptops
    - Use complex password, encrypt disk, enable timeout

Harvard Requirements and How To's, contd.

- Patch system & applications
  - How to configure for automatic patching
- Encrypt communications with servers
  - Configure to require encrypted connections with servers (e.g. mail, calendar, VoIP, IM, fileshare (where possible))
- Protect contents if device stolen or lost
  - Encrypt device, enable remote wipe

Harvard Requirements and How To's, contd.

- Report loss, theft or improper use of devices

  How to report security incident

- Annually scan devices for HRCI

  How to use a scanning application to look for SSNs and credit card numbers

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
2	http://web.mit.edu/6.111/www/s2007/LABS/LAB4/lab4.pdf
2	MIT logo
3	https://security.harvard.edu
4, 6	http://security.harvard.edu/use-strong-passwords
5	http://features.en.softonic.com/which-password-manager-should-you-use-1password-dashlane-or-lastpass
7-10	http://security.harvard.edu/know-your-data
11-13	https://security.harvard.edu

Safe computing

Last words

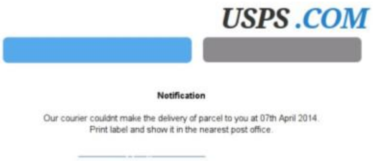
CSCI E 45b: The Cyber World – part B

Pay attention, #1

- Don't get phished

  Think hard about any email message you receive that asks you to click on a link, or any other action "quickly"

  e.g. US Post Office telling you to print out a claim form



USPS.COM

Notification

Our courier couldnt make the delivery of parcel to you at 07th April 2014.
Print label and show it in the nearest post office.

Pay attention #2

- Think about your future

  Think hard about what you want to post on a social media site

  I'm leaving for 3 weeks in the Alaska back country, no net, no phone.

  I stopped off at a bar on my way back from the drunk driving hearing, got well buzzed.

  Those Anonymous guys are real jerks.

  My boss will never figure out where the money went.

  Think about what sites you visit, what content you look at

GOOD JUDGEMENT COMES FROM EXPERIENCE. EXPERIENCE COMES FROM BAD JUDGEMENT.
Jim Horning
PICTUREQUOTES.COM

Pay attention #3

- Be up to date on the rules

Watch the Internet governance discussion

Tomorrow's Internet may be very different than today's

Watch the legal developments

Will there be any limit to government or corporate surveillance?

Watch the regulatory developments

Will the FCC's new rules cause normal Internet service to degrade?

Think about who you do business with

Will there be any limit to Google's surveillance?

Pay attention #4

- Protect your computer

Do not surf porn sites using your work computer

Do not click on URLs in email that wound up in your junk mail folder

Do not plug found thumb drives (or any other device) into a computer you care about

Pay attention #5

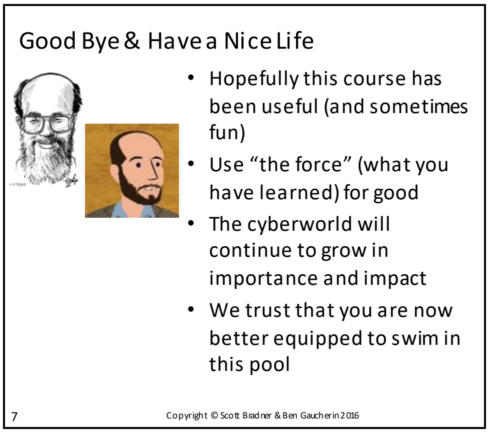
- Be a good information steward

It is 10 PM, do you know where your data is?

Keep track of where all of your confidential information resides

Use secure erase on the disk when you dispose of a computer

Never put unencrypted confidential information on portable media



Good Bye & Have a Nice Life

- Hopefully this course has been useful (and sometimes fun)
- Use "the force" (what you have learned) for good
- The cyberworld will continue to grow in importance and impact
- We trust that you are now better equipped to swim in this pool

7

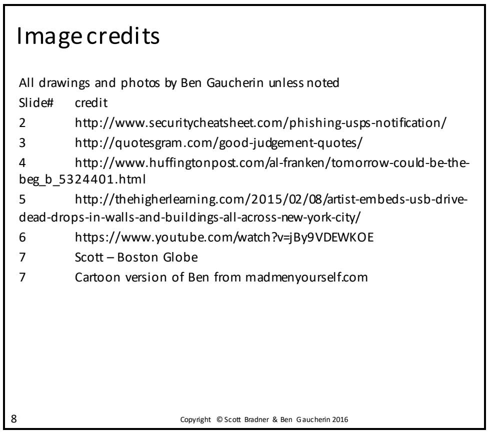


Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
2	http://www.securitycheatsheet.com/phishing-usps-notification/
3	http://quotesgram.com/good-judgement-quotes/
4	http://www.huffingtonpost.com/al-franken/tomorrow-could-be-the-beg_b_5324401.html
5	http://thehigherlearning.com/2015/02/08/artist-embeds-usb-drive-dead-drops-in-walls-and-buildings-all-across-new-york-city/
6	https://www.youtube.com/watch?v=jBy9VDEWKOE
7	Scott – Boston Globe
7	Cartoon version of Ben from madmenyourself.com

8