Change & Opportunity II

Scott Bradner
ABCD
December 3, 2010

A World of Change

- changes at Harvard
  - technology security & other
- changes elsewhere
  - that matter to IT

Harvard

- technology security changes since last year
  - very minor tweak to HEISP
  - tweak to confidential information definition
  - remote access policy
  - receiving HRCI via email
  - travelers advisory
  - breach reporting
  - approval of HRDSP
- organizational changes
  - on their way

HEISP

- Harvard Enterprise Information Security Policy
- covers all confidential information at Harvard
  - and all people who deal with confidential information
  - new - separate policy for research data (HRDSP)
- set of high-level policies
  - implementation is local (products etc)
- annual compliance process
  - includes self assessment questionnaire (SAQ)
  - tweaks to SAQ
    - some “and used” clauses changed
    - encrypting backups that include HRCI now required

abcd change 4

Is My Information Confidential?

- common question - a sample logic flow
  - 1 - is the information about identifiable people?
    - No - go to Harvard info
  - 2 - is the information Directory Information?
    - Yes - go to directory info
  - the information is confidential
  - 3 - does the information include HRCI (e.g., SSN)?
    - Yes - the information is HRCI
  - Harvard Info - would The Crimson care?
    - Yes - the information is confidential
  - directory info - privacy flags (including FERPA) on?
    - Yes - the information is confidential

abcd change 5

Confidential Information Deff.

- security.harvard.edu -> glossary
- complaint - could be seen as restricting people from talking about their own pay or from reporting non-compliance
- fix - add:

  "This policy is not intended to prohibit employees from disclosing their own personal information, such as salaries or other terms and conditions of employment to whomever they please, nor anyone from reporting compliance issues to proper authorities."

abcd change 6

Remote Access Policy

- required by Mass regulations
- decided to focus on SSNs
  - most common HRCI data element
- policy: each application owner must ensure
  - 1 - only people with a business need are to be given permission to remotely access SSNs
    - individual permission, not role - keep record of approvals
  - 2 - if permitted, must know to use one of:
    - a - Harvard owned & maintained computer (encrypted etc.)
    - b - terminal server interface to application
    - c - "system on a stick"

abcd change 7

Remote

- "remote" is defined as 'not connected to the Harvard wired network'
  - using your smart phone or WiFi-connected laptop in your office is remote
- VPN does not override above

abcd change 8

Receiving HRCI via Email

- security.harvard.edu -> resources -> advisories
- Mass regulations: must not send someone's SSN via unencrypted email
  - corollary: must not have process that requires someone to send you their SSN via unencrypted email
- but some people send HRCI even if not requested
  - SSNs, credit card #, drivers license #s, etc.

abcd change 9

Receiving HRCI via Email, contd.

- case 1 - if HRCI not needed (SSN as example)
  respond (not including the original message)
  "I am not permitted to receive SSNs in unencrypted email. I have deleted your message. Please re-send with no SSN."
- case 2 - HRCI needed but not via email
  respond (not including the original message)
  "I am not permitted to receive SSNs in unencrypted email. Following standard Harvard practice, I have destroyed your original message containing this information.
  You may re-send using the right process, which is to transmit this information by FAX." (or whatever process)

abcd change 10

Travelers Advisory

- security.harvard.edu -> resources -> advisories
  -assume laptop (smart phone, etc.) will be lost
  encrypt device if any confidential information (no HRCI)
  securely upload any generated information
  remove confidential info after transfer verified
  -US law: must not export encryption technology to:
  Cuba, Iran, North Korea, Sudan, or Syria
  -local restrictions on encryption in some countries
  -you may have to tell your password to authorities
  -US can (and does) search devices at border
  -register your international travel with I-SOS

abcd change 11

Breach Reporting

- security.harvard.edu -> resources -> advisories
- when a breach is known or suspected
  breach examples: lost/stolen computer, lost smartphone, intrusion into a system, improper posting, misdirected email, ...
  note: reporting requirement applies to all cases where unencrypted Harvard confidential information is involved, not just where the device is owned by Harvard
  you are on your own if it was just your own tax return
  breaches of HRCI must always be reported, even if encrypted
  note: storage of HRCI on any user device is prohibited

abcd change 12

Breach Reporting, Process

- immediately notify school/university CIO office
  or security officer
- immediately notify OGC, UTSO & UCIO if breached data might require legal notification
  e.g., HRCI, student data
- remediate & investigate
  take system off line, start forensics, understand data
- within 72 hours - develop incident report
  provide to OGC, UCIO & UTSO if reportable data
- if reportable data - UCIO forms response team

abcd change 13

Breach Reporting, Notifications

- UCIO response team includes University and local unit press officials
- OGC determines if legal notifications required
- OGC works with local unit to develop notices
- local unit responsible for all costs
- UTSO reviews incident to see if HEISP needs to be updated
- detailed response process and report templates under development

abcd change 14

HRDSP

- Harvard Research Data Security Policy
  special tab on security.harvard.edu
- approved in August & distributed by Provost
- applies to all non-public research data at Harvard
  does not apply to affiliated institutions
- some data from non-Harvard sources subject to a "data use agreement" (DUA)
  defines requirements for access to and protection of data
- some grants and contracts also include DUAs

abcd change 15

Data Use Agreements

- individual researchers do not have the authority to sign a DUA for Harvard
  - authorized signers are the sponsored project offices
  - signers will check with school CIOs to see if researcher can meet data protection requirements
- if there is a DUA, then the requirements in it govern, unless they are seen as too weak

abcd change 16

Institutional Review Boards (IRBs)

- by federal law human subject research at Harvard must be reviewed by an IRB
- Harvard has 3 IRBs
  - Medical & Dental School, SPH and rest of University
- human subject research means
  - research involving interacting with people
    - interactive experiments, surveys, medical studies, etc.
  - research involving information about people
    - databases of student records, raw census data, network monitoring, etc.

abcd change 17

Research Data Levels

- IRB works with each researcher to categorize their research data into levels
  - level 5 - extremely sensitive information about people
  - level 4 - very sensitive information about people
  - level 3 - sensitive information about people
  - level 2 - benign information about people
  - level 1 - non-confidential information
- information not about people can still be confidential
  - e.g., information with national security implications should be classified as level 4

abcd change 18

HRDSP, contd.

- levels
  - level 5 - new, data requiring very special protection
  - level 4 - existing, HEISP HRCI
  - level 3 - existing, HEISP other confidential information
  - level 2 - new, minimal risk info
  - level 1 - existing, HEISP public information
- protection requirements from HEISP
  - specific lists adapted from HEISP SAQ
  - level 5 special - must not be on a net, etc.

What Level is the Right Level?

1 - is there a meaningful DUA?
  yes - the DUA governs protection requirements
2 - is the information national security information?
  Yes - the information is Level 4
3 - is the information about identifiable people?
  No - the information is Level 1
4 - are people's lives are risk if information disclosed?
  Yes - the information is Level 5
5 - is the information medical or include HRCI?
  Yes - the information is Level 4
6 - is the information benign?
  Yes - the information is Level 2
  otherwise the information is Level 3

Legal Requests for Research Info.

- if you get a:
  - subpoena
  - National Security Letter
  - court order
  - Freedom of Information Act (FOIA) request
- tell the sender that you are not authorized to accept it - tell the sender to talk to OGC
  - because you are not authorized to accept any such request or respond to one
- consider getting a Certificate of Confidentiality
  - IRB can help you get one

Organizational Changes

Figure 1. Transition Program Structure

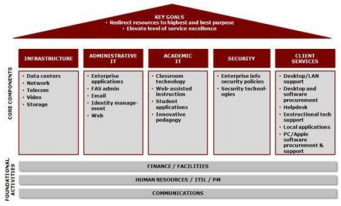


Figure 3. Transition Timeline

abcd change 22

Changes in the Real World

- many IT-related changes in process in the non-Harvard world
- some will impact Harvard
- most will impact you & me
- just a few of them

abcd change 23

The End of the (Old) Internet #1

- pool of unused IP addresses managed by the Internet Assigned Numbers Authority (IANA)
- total pool: 255 "/8s" (17 M addresses each)
- IANA assigns /8s to regional IP registries (RIR) based on need - there are 5 RIRs

  RIRs assign smaller blocks of addresses to ISPs
- IANA assigned 4 /8s on Tuesday - leaving 7
- when number left gets to 5, each RIR gets assigned one, and then there are none

  this could happen by the end of the year or early next

abcd change 24

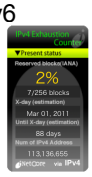
End #1, contd.

- the RIRs will take a while to assign the space to ISPs
  - this could happen by mid next year for some RIRs
- at that point there will be no "new" IP addresses
- the RIRs have developed "transfer" policies
  - will permit buying and selling of IP address blocks
  - but the effect may be limited
- new or expanding use of the Internet with IPv4 will be constrained

abcd change 25

End #1, contd.

- network address translators will help some
  - permit multiple computers to use same address
- real solution - move to next generation of Internet Protocol - IPv6
  - 4 B times the address space
- current generation PC OSs support IPv6
- Harvard will have to start enabling and supporting IPv6 within a few years



http://www.potaroo.net/tools/ipv4/index.html

abcd change 26

The End of the (Old) Internet #2

- an end that did not happen (yet)
- last year I mentioned the ITU was
  - attempting to take over control of the Internet
  - put control in the hands of government regulators
- big fight in ITU meeting in Mexico in October
  - 3-week meeting to plan for the next 4 years of the ITU
  - many proposals for ITU takeover
  - all modified to seemingly not enable takeover
  - but will depend on ITU staff interpretation of final text
- but expect the ITU will be back

abcd change 27

The End of the (Old) Internet #3

- The Federal Communications Commission announced Tuesday that it would vote on "network neutrality" on Dec 21st
  - actual proposal not public yet
- network neutrality is what the Internet has had for its whole existence
  - no permission needed to deploy new services
  - no special handling of particular traffic
    - e.g., data from ISP business partners
  - resulted in an explosion of applications

abcd change 28

End #3, contd.

- FCC proposal seen as a mixed bag
  - telling that the heads of the carriers like it
- republicans hate it
  - want "no regulation" so 'to preserve the growth of the Internet'
  - but can not see above the physical interconnect
    - only see the Internet as "a series of tubes"
    - can not see the services that use the Internet - Google etc.
- FCC plan mostly exempts wireless from regulation
- carriers have an incentive to be unfair
  - charge extra for "good" service

abcd change 29

End #3, contd.

- if no regulation, expect carriers to ramp up interfering with traffic
- regulation may specifically enable wireless carriers to interfere with traffic
- republican congress could do the same for wired carriers
- create a protection racket
  - it would be a shame if your bits were to get lost...

abcd change 30

The End of the (Old) Internet #4

- growth of video straining old Internet cooperation
- most ISPs have cost-shared peering with other ISPs of similar size
  - as long as a general balance in traffic
- video is distorting traffic balance - will lead to new fees & some disruptions
  - e.g., Comcast vs. Level 3 (Netflix)

comcast Level(3) COMMUNICATIONS NETFLIX

abcd change 31

Privacy?

- FTC proposing a 'do not track' flag
  - too little, to late
- WSJ series on Internet user tracking
  - "they" know whatever you do on-line
  - deep packet inspection on the rise in ISPs
  - computer fingerprinting bypasses cookies
  - Google knows all
  - third party ad systems know more than Google
  - anyone can subpoena whatever "they" know
    - the Feds can just ask (using NSLs)

abcd change 32

Privacy?, contd.

- Internet advertising - $25 B/year
  - e.g., BlueKai trades data on more than 200 million Internet users

Data Rules! And We've Created the Largest Marketplace for it.

BlueKai's data-centric approach to audience targeting has made the marketer's dream of "reaching an audience anytime anywhere" a reality.

We created a marketplace where buyers and sellers trade high-quality targeting data like stocks, while ensuring transparency and control for consumers. Supported by BlueKai's proprietary platform, this marketplace is an open exchange for all audience data. Most importantly, it's anchored by BlueKai Intent™, the largest aggregation of in-market shopping data available on the Internet.

BlueKai. Creating a new data economy.

bluekai

abcd change 33

Government Control

- US government seized 82 domain names of sites that they claimed were violating copyright
  - had no real effect since websites were still running and quickly got new domain names
- Combating Online Infringement and Counterfeits Act (COICA) bill in congress
  - would require ISPs to block access to list of websites created by government
  - could cause very large disruptions if filter on IP addresses
    - one IP address can support 100 K websites
  - useless to filter on domain name - just get new name

abcd change 34

Paywalls

- content owners having a hard time working out Internet-age business models
- keep trying to use old physical-world models
  - e.g., DMCA with music & movie sharing
- latest is newspapers erecting "paywalls"
  - e.g., Murdoch's papers including THE TIMES
  - soon The New York Times
- pay to read
- likely to fail - too many other sources of news
- some will succeed - e.g., THE WALL STREET JOURNAL.

abcd change 35

New TLDs

- coming soon to an Internet near you
  - .IPaidForThisTLD
- ICANN will soon be selling top level domains
  - to compete with .com, .net, .org & .edu
- for just $185,000 we could get ".harvard"
  - and could have www.harvard
- likely to cause considerable confusion

abcd change 36

Enough for Now

- these have been a few of the changes that are underway
  at Harvard and “out there”

have fun living through them

(see you next year)

abcd change 37

abcd change 38