


Information Security Strategy, Classification, Policy, and Mindset
Introduction

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016




Introduction: learning goals



- Explore the key elements of what sets the foundation for Information Security in an organization: strategy, classification, policies, etc.

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Topics, all required



- Information security strategy – R
Strategy as a key foundation to information security
- Classification – R
Triaging data and other key assets
- Policies & policy making – R
Overview of what policies are and their importance to an organization

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Topics, all required



- Harvard's information security policy – R
An example of information security policy
- Information security programs – R
Implementing the strategy
- Security and the hacker mindset – R
Exploring the twisted mindset of security professionals, and the importance of hacking

4

Copyright © Scott Bradner & Ben Gaucherin 2016

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 <https://www.linkedin.com/pulse/rout-planning-out-planning-strategy-reggie-legend>
- 3 <http://security.harvard.edu/know-your-data>
- 3 <http://www.ereMEDIA.com/tint/do-old-school-workplace-rules-and-hierarchies-still-matter/>
- 4 <http://security.harvard.edu>
- 4 <https://www.flickr.com/photos/drbeXl-/4414113538/in/photostream/>
- 4 <https://americascienceblog.com/2013/09/>

5


Copyright © Scott Bradner & Ben Gaucherin 2016

Information Security Strategy, Classification, Policy, and Mindset
Information security strategy

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016

What it is, and why it matters




- Strategy helps define...
 - Where** we are going
 - Why** we are going there and why it is a better place
 - Why we are going anywhere: problem to solve, opportunity to seize
 - How** we are going to get there
 - What options/paths exist to get there, which one is the best option/path, and why

2 Copyright © Scott Bradner & Ben Gaucherin 2016

What it is, and why it matters, contd.

- As a result, strategy documents are important communication tools to:
 - Communicate to a broad set of senior leaders...
 - ...on a topic they may not know much about...
 - ...in a way that they understand, can relate to, and ultimately can support
 - Communicate to the people who are going to do the work:
 - The critical backdrop for all of the work they will be doing
 - The guideposts to validate if the work done will fulfill the strategy



3 Copyright © Scott Bradner & Ben Gaucherin 2016

Other important aspects of strategy

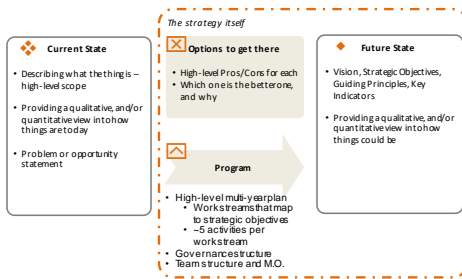


- Things change all the time, as a result...
The future will not be exactly what you thought it was going to be
You need to review your strategy, assumptions, and program regularly to potentially course correct
- It is not an exercise in precision, rather it is achieving consensus on the general direction and broad parameters

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Four easy steps




5

Copyright © Scott Bradner & Ben Gaucherin 2016

The following are extracts from an early draft of Harvard's Information Security strategy

6

Copyright © Scott Bradner & Ben Gaucherin 2016

Information Security Vision & Scope 


Vision

*To make **everyone** at Harvard a good steward of confidential information*

Scope

- **Everyone:** faculty, staff, students, affiliates, contractors and everyone else who handles our information or uses Harvard's infrastructure for information storage or processing (e.g. our networks, systems and/or applications)
- **Information:**
 - Information of any kind (e.g. research data, administrative data, etc.) and in whatever form it may be (electronic, paper or verbal)
 - And implicitly the systems that process this information (e.g. computers, networks, paper storage, etc.)


Copyright© Scott Bradner & Ben Gauderin 2016 7

Information Security Goals 

What does it mean for everyone to be a good steward?

- Everyone at Harvard is aware of, and follows good information handling and safe computing practices
... and these are fully integrated into the way everyone does business
- Everyone at Harvard is aware of privacy requirements and expectations
- We have a shared understanding of the risks we are explicitly or implicitly accepting and who is accountable for each
- We have University-wide resources available and useful to all
 - A central security team, responsible for a Security Operations Center and delivering services to the schools
 - A Harvard Information Security Policy (HISP), shared Standard Operating Procedures and documented Best Practices
 - A common understanding of the applications and systems that support critical business processes and a reference architecture for ensuring their availability
- We have a way to measure and assess our progress on an ongoing basis
- There are consequences to not being a good steward of Harvard's information


Copyright© Scott Bradner & Ben Gauderin 2016 8

Information Security Program Attributes 

Risk-Based	
<p><i>What we mean</i></p> <ul style="list-style-type: none"> • Our allocation of resources, attention and controls is aligned with the impact and likelihood of a risk • We will all understand the risks we are explicitly or implicitly accepting 	<p><i>Why</i></p> <ul style="list-style-type: none"> • This is a proven approach in the information security space that extends and leverages the University risk management structure/process
People-Centric	
<p><i>What we mean</i></p> <ul style="list-style-type: none"> • We must educate, empower and entrust all members of the Harvard community to be able to recognize and adequately protect sensitive information 	<p><i>Why</i></p> <ul style="list-style-type: none"> • Harvard is by design an open environment, therefore an information security program needs to balance the necessity for controls with the mission of the University • At Harvard, the success of an information security program depends on the "collective action" by the community at large as a simple mistake or oversight by a single individual could have severe negative consequences

Copyright© Scott Bradner & Ben Gauderin 2016 9

Information Security Metrics



To assess the effectiveness of our program we will...


- Measure progress in reducing the impact of external threats
 - Major: Reportable breaches
 - Smaller: Virus/malware infections
- Measure progress in raising internal awareness
 - Percentage of community who acknowledge Confidentiality Agreement
 - Percentage of community who make use of educational resources

Our approach will utilize...

- Objective criteria such as the Cyber Security Index
- Peer institution benchmarks
- Informed first-hand reports from CIOs

Copyright © Scott Bradner & Ben Gaucherin 2016 10

Information Security Program Components




The following three-pronged approach will allow us to both clarify the responsibilities of individuals, as well as guide decisions at a macro level regarding projects/initiatives aimed at improving Harvard's Information Security:

	Aware	Protected	Ready
Individual	<ul style="list-style-type: none">• Know good information handling and safe computing practices• Understand what type of information you handle• Know what to do with the information you handle	<ul style="list-style-type: none">• Use good information handling and safe computing practices	<ul style="list-style-type: none">• Know what to do in case of an incident
Institutional	<ul style="list-style-type: none">• Detection technologies• Security Operations Center• Participation in collaborative and information sharing efforts (e.g. ACSC)	<ul style="list-style-type: none">• Firewalls, anti-virus/malware, secure gateways• Security Operations Center• Standards for system and application patching, hardening and availability	<ul style="list-style-type: none">• Establish proper policies• Have standard operating procedures• Relationships with OGC and Law Enforcement

Copyright © Scott Bradner & Ben Gaucherin 2016 11

Strategy update



- Harvard's Information Security strategy continues to evolve
- The strategy defines the elements of the programs
 - New data classification
 - Overhauled policies
 - Awareness campaign

12 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted


Slide#	credit
2	https://www.linkedin.com/pulse/rout-planning-out-planning-strategy-reggie-legend
3	http://news.harvard.edu/gazette/story/2011/06/for-harvard-an-it-summit/
4	http://huit.harvard.edu/harvard-cio-council
12	http://security.harvard.edu

Information Security Strategy, Classification, Policy, and Mindset
Classification

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016


Data classification



- “Data Classification is the conscious decision to *assign a level of sensitivity* to data as it is being created, amended, enhanced, stored, or transmitted. The classification of the data should then *determine the extent to which the data needs to be controlled / secured* and is also *indicative of its value in terms of Business Assets.*”
www.yourwindow.to

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Data classification, contd.



- Information sensitivity levels are an important factor in assessing risk
If everything is “Top Secret”, then nothing is special, and everything is treated the same

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Harvard's data classification levels

Level 3 - Information that could cause risk of material harm to individuals or the University if disclosed

- Information that includes HUIDs
- University financial information
- Employee records that do not include SSNs or bank account numbers
- Non-directory student information
- Directory information for students with a FERPA block

7 Copyright © Scott Bradner & Ben Gaucher in 2016

Harvard's data classification levels, contd.

Level 4 - Information that would likely cause serious harm to individuals or the University if disclosed

- Credit card numbers
- Social security numbers
- Passwords
- Personally identifiable genetic information
- Personally identifiable healthcare information
- Student financial information

8 Copyright © Scott Bradner & Ben Gaucher in 2016

Harvard's data classification levels, contd.

Level 5 - Information that would cause severe harm to individuals or the University if disclosed.

- Research data classified by an IRB as Level 5
- No administrative data known to be level 5 to date

9 Copyright © Scott Bradner & Ben Gaucher in 2016

Harvard's data classification levels, contd.

LEVEL 1	Public information
LEVEL 2	Level 2 is information the University has chosen to keep confidential but the disclosure of which would not cause material harm.
LEVEL 3	Level 3 information could cause risk of material harm to individuals or the University if disclosed.
LEVEL 4	Level 4 information would likely cause serious harm to individuals or the University if disclosed.
LEVEL 5	Level 5 information would cause severe harm to individuals or the University if disclosed.

For all levels:
Research data classified by an IRB as Level n
Information subject to a data use agreement that specifies a protection level best met by Level n classification

10 Copyright © Scott Bradner & Ben Gaucherin 2016

Systems classification

With data classification we have:
Confidentiality
Integrity
Availability

Add System classification and we have:
Confidentiality
Integrity
Availability

- Recently, Harvard realized that data classification alone is no longer sufficient
- We have systems with data that ranks low on the data classification scale, but whose failure/compromise would have significant impacts
E.g., garage control systems, food refrigeration systems, etc.
- So we are developing a parallel classification for systems

11 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide#	credit
2	http://www.onsocialmedia.org/blog
3	http://www.linkedininiches.com/top-secret/
4	http://www.titus.com/titus-blog/2010/09/information-marking-for-greater-security-awareness/
5-10	http://security.harvard.edu/know-your-data
10	http://www.nydailynews.com/news/world/northern-ireland-sue-ira-interviews-article-1.1802987


12 Copyright © Scott Bradner & Ben Gaucherin 2016

Information Security Strategy, Classification,
Policy, and Mindset
Policies, and policy making

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016


Policy



- Policies are rules to guide decisions and actions to achieve a plan, goal
 - Made by organizations
 - To guide their own behaviors
 - In the IT world, policies result in limitations to access to, and distribution of information, as well as constraints on the activities of individuals
 - Organization based disciplinary implications if not followed/complied with

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Policy, contd.



- Laws and regulations
 - Are also rules
 - Made by the executive and legislative branches of governments
 - To “guide” the behaviors of companies, and citizens
 - Legal penalties if not followed/complied with

3 Copyright © Scott Bradner & Ben Gaucherin 2016

How do policies come to be?



1. **Explicit policy development process**
Most common source in an organization
Management issues policies to ensure decisions are made in a way that is consistent with management's objectives
2. **Un-expected situations**
When a situation arises that does not have policies to support its handling
Or when current policies seem unfit to handle some cases

4

Copyright © Scott Bradner & Ben Gaucherin 2016

How do policies come to be?, contd.



3. **Implied**
Policies that are not stated but implied by the way an organization handles a situation important in a legal liability context
Comparing your implied policy to a standard of due care
4. **Externally imposed**
Government regulations – e.g., HIPAA, export limitations
Industry – e.g., PCI-DSS
Convenient for local policy makers

5

Copyright © Scott Bradner & Ben Gaucherin 2016

Art and science of policy making

- **Not too high-level**
Ultimately any set of information security policies can be reduced to a single high-level policy



The Goldilocks principle

- e.g., "Everyone is expected to protect the information of the organization"
- **Not too specific**
Too specific a statement prevents understanding the philosophy of protection, and its applicability to new situations

6

Copyright © Scott Bradner & Ben Gaucherin 2016

Art and science of policy making, contd.



Example of technology specific policy:
Thou shall not kill people with axes

- Few exceptions
Any exception, challenges the validity/rationale for the rule
- Should be technology agnostic
Technologies will come and go, and your policy needs to withstand the test of time.
- It needs to be practical and actionable
People need to be able to actually do what they are expected to do, AND they need to know how to do it

7

Copyright © Scott Bradner & Ben Gaucherin 2016

Art and science of policy making, contd.



- Need more than just a policy statement
A policy statement alone is not sufficient. Understanding scope of applicability, roles, etc. provides context, clarifies how the policy should be applied and the accountability of failing to follow the policy
- Bottom line, you want people to:
Know they need to follow them
Be able to follow them
Not have to guess in the "heat of battle"

8

Copyright © Scott Bradner & Ben Gaucherin 2016

Use clear language



The man who defined MUST

- RFC 2119 – Bradner 1997
- **MUST**
This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- **MUST NOT**
This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

9

Copyright © Scott Bradner & Ben Gaucherin 2016

Use clear language, contd.

MUST
MUST NOT
SHOULD
SHOULD NOT
MAY

"SHOULD is a *MUST* with an escape clause" © - Scott

- **SHOULD**
This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT** use **SHOULD**

10

Copyright © Scott Bradner & Ben Gaucherin 2016

Use clear language, contd.

MUST
MUST NOT
SHOULD
SHOULD NOT
MAY

- **SHOULD NOT**
This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- **SHOULD NOT** use **SHOULD**
NOT

11

Copyright © Scott Bradner & Ben Gaucherin 2016

Use clear language, contd.

MUST
MUST NOT
SHOULD
SHOULD NOT
MAY

- **MAY**
This word, or the adjective "OPTIONAL", mean that an item is truly optional. [...]

12

Copyright © Scott Bradner & Ben Gaucherin 2016

Policy reviews



- Policies should be reviewed regularly and after incidents
- Policies change more slowly than the conditions that lead to them
- Unfortunately, it leads to time lag between condition change and policy change
People need to know what to do when they are faced with a situation where the current policies don't fit

13

Copyright © Scott Bradner & Ben Gaucherin 2016

Policy reviews



- Policy reviews allow:
The elimination of obsolete policies
The re-stating, re-framing of policies
- Many regulations require that you review your policies when a major incident occurs

14

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

- | Slide# | credit |
|--------|---|
| 2 | http://www.writergirl.com/5-leadership-tips-from-a-public-policy-officer/ |
| 3 | http://blogs.loc.gov/law/2015/04/interview-with-gail-warren-virginia-state-law-librarian/ |
| 4, 5 | http://www.eremedia.com/tnt/do-old-school-workplace-rules-and-hierarchies-still-matter/ |
| 6 | https://valleybusinessreport.com/wp-content/uploads/2017/10/Goldilocks.jpg |
| 7 | http://www.rustafied.com/tools-skills-stats-and-summaries/ |
| 8 | http://www.eagleeyenetworks.com/video-api-example-code/ |
| 9 | https://www.sobco.com |
| 13, 14 | http://pdsh.wikia.com/wiki/Father_Time |

15

Copyright © Scott Bradner & Ben Gaucherin 2016

Information Security Strategy, Classification, Policy, and Mindset
Harvard's information security policy

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016

Structure

- **Policy statement:**
The actual policy statement
- **Requirement(s):**
Requirement(s) to fulfill the policy
- **How To('s):**
Specific How To('s) for a specific environment, set of tools, etc. to fulfill a requirement

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Structure, contd.

- **Clear separation between policy statements, requirements and How To's**
People more likely to go to requirements and How To's

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Policy statements walk-through



HARVARD
Information Security

- 15 statements to cover the entirety of requirements/needs to protect information
- Not limited to electronic information
- Informed by legal and compliance requirements on the institution:
State of Mass. 201 CMR 17, FERPA, etc.

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Expectations of people



- All users are responsible for protecting Harvard confidential information that they use in any form from unauthorized access and use.
- All users are responsible for protecting their Harvard passwords and other access credentials from unauthorized use.

5

Copyright © Scott Bradner & Ben Gaucherin 2016

Expectations of people, contd.



- All persons accessing Harvard confidential information must be trained in protecting such information.
- All users of Harvard confidential information resources must be accurately and individually identified.

6

Copyright © Scott Bradner & Ben Gaucherin 2016

Expectations concerning systems



- **Software must be kept up to date** on all computers and devices that process or store Harvard confidential information.
- All servers storing Harvard confidential information must be **protected against improper access**.

7

Copyright © Scott Bradner & Ben Gaucherin 2016

Expectations concerning systems, contd.



- All servers and locations where Level 4 or 5 information is stored must be **accurately identified and physically secure**.
- There must be a mechanism to **limit the number of unsuccessful attempts** to log into an application or server that processes or stores Harvard confidential information.

8

Copyright © Scott Bradner & Ben Gaucherin 2016

Transporting, disposing information



- Electronic and physical records containing Harvard confidential information must be appropriately **protected when transported or transmitted**.

9

Copyright © Scott Bradner & Ben Gaucherin 2016

Transporting, disposing information, contd.



- Electronic and physical records containing Harvard confidential information **must be properly disposed of** so that the information cannot be retrieved or reassembled when no longer needed or required to be kept.

10

Copyright © Scott Bradner & Ben Gaucherin 2016

Other expectations



Massachusetts regulations require Harvard to "be convinced" that the third party is capable of protecting the information

- Harvard must conduct appropriate due diligence to ensure that **third parties** that store or have access to Harvard confidential information **are capable of properly protecting the information and must require such third parties to protect the information.**

11

Copyright © Scott Bradner & Ben Gaucherin 2016

Other expectations, contd.



- **Any actual or suspected loss, theft, or improper use of or access to**, Harvard confidential information **must be reported as soon as possible** to a Local Information Security Officer, the University Chief Information Security Officer and the Office of General Counsel.

Harvard contracts for an anonymous/whistleblower reporting service

12

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted


Slide#	credit
4	http://security.harvard.edu
5, 6	http://catchthewave.seas.harvard.edu/
7, 8	http://huit.harvard.edu
9	http://www.goblinsforum.com/viewtopic.php?f=3&t=1509&start=5
10	http://www.monomachines.com/shop/paper-digital-shredders/paper-shredders.html
11	http://www.zazzle.com/third+party+gifts
12	http://www.keepcalm-o-matic.co.uk/p/if-you-see-something-say-something/

Information Security Strategy, Classification, Policy, and Mindset
Information security programs

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016


Security program



- Program to build and maintain the necessary support infrastructure (people/policy/process/tools) to support a community of users in the protection and proper use of organizational information assets

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Security program, contd.



- The security program is driven by the Chief Information Security Officer (CISO), but owned by the top leader in the organization (e.g. CEO)
If the CISO reports to the CIO, information security will be viewed as an IT thing...
...unless the CEO takes a very visible role in the information security program

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Key elements



- Not a one time thing – involves continuous risk assessment, policy definition and mitigations
- Governance and compliance structure
 - Roles and responsibilities, what decisions get made by whom, what are the consequences for not following policy, etc.
 - e.g., yearly compliance letter/questionnaire process, process for official opinions/decisions, sanctions

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Key elements, contd.



Parisa Tabriz
Google Security Princess

- Standard operating procedures (beyond How To's)
 - e.g., crisis management and incident response processes, after action review process, etc.
- Establish designated security staff, expertise, tools –and availability expectations
 - e.g., centralized security team, vulnerability assessment tools, 24x7, etc.

5

Copyright © Scott Bradner & Ben Gaucherin 2016

Key elements, contd.



**Small Actions.
Big Difference.**
You help keep Harvard secure.

- On-going communication and awareness program
 - Communication to users, and various sub-groups within the organization
 - e.g., awareness and training programs, general communication campaign, advisories, etc.
- On-going assessment of security program/policy effectiveness
 - e.g. metrics program, internal/external audits, etc.

6

Copyright © Scott Bradner & Ben Gaucherin 2016

Getting people to do the right thing



- Awareness is not training
Training is about particular procedural change
Awareness is about consciousness raising
- Usability and security
As seen in the usability module, usability plays a major part in user compliance
- Reducing the risk of “plausible deniability”
If there is not explicit statement of policy, then the user can legitimately claim they did not know what was expected of them

7

Copyright © Scott Bradner & Ben Gaucherin 2016

Getting people to do the right thing, contd.



- Even if it is in the “manual”, how do you ensure your users are reading the manual
- Making the value of information stewardship personal
Protecting “my stuff”
Corporate info = my stuff
Fear of consequences
Appealing to a sense of duty
- Use propaganda techniques
See propaganda techniques on Wikipedia

8

Copyright © Scott Bradner & Ben Gaucherin 2016

Getting people to do the right thing, contd.



- Be aware of the different messages for different communities
General users, sys admins, developers, etc.
- Be careful, what you say and how you say it
E.g., “crying wolf” (because of flawed risk analysis) will get people to ignore you, because everything is treated as a high risk - therefore nothing is actually seen as high risk

9

Copyright © Scott Bradner & Ben Gaucherin 2016

Getting people to do the right thing, contd.



- The “right” level of accountability and consequences
 - Enforcing accountability too strongly might drive the wrong behavior (e.g. not surfacing security breaches)
 - Enforcing too lightly, conveys the message that there are no consequences
 - And enable anonymous whistleblowers
 - Legally required in the US for publically traded companies

10

Copyright © Scott Bradner & Ben Gaucherin 2016

Security as a collective action problem

- **Collective action problem**
 - No one can solve this alone
 - Everyone needs to do “their part”
 - Any weak links puts everyone at risk



11

Copyright © Scott Bradner & Ben Gaucherin 2016

Security as a collective action problem



- **Tragedy of the commons**
 - Rules when sharing a limited resource (or achieving a collective action goal)
 - Things are best if everyone complies
 - And things may be ok if some people “cheat” a little, some of the time
 - But things will definitely fail if some people “cheat” in a big way and/or too regularly. Or if too many people cheat

12

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide# credit

- 2 http://www.campussafetymagazine.com/article/friday_humor_6_major_security_fails/slideshow
- 3 <http://www-03.ibm.com/security/qa/en/ciso/>
- 4 <https://memegenerator.net/instance/53464097>
- 5 <http://www.telegraph.co.uk/technology/google/11140639/Googles-top-secret-weapon-a-hacker-they-call-their-Security-Princess.html>
- 6 <http://security.harvard.edu/2015AwarenessQuiz>
- 7 <http://www.cnet.com/news/ashton-kutcher-suffers-twitter-hack-attack/>
- 8 <https://www.flickr.com/photos/drbeal/4414113538/in/photostream/>
- 9 <http://freebeacon.com/blog/the-cost-of-crying-racism-ctd/>
- 10 <https://lemurking.wordpress.com/2008/02/14/loose-lips-sink-ships-or-worse/>
- 11 <http://andersonleadershipsolutions.com/leaders-who-sets-the-standards/weak-link/>
- 12 <http://tragedy.sdsu.edu/>
- 13


Copyright © Scott Bradner & Ben Gaucherin 2016

Information Security Strategy, Classification, Policy, and Mindset
Security and hacker mindset

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016



Schneier on the “security mindset”



- Looking at the world differently than most people
- Creative thinking on ways to subvert, abuse the system
 - “Being security conscious means being a criminal, if only in one’s head, and this spooks people.” – anonymous comment
- “Paranoia is a mechanism”
- Usefulness not limited to security
 - Law making, policy making ;), system building, etc.

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Misguided information security thinking



- Good guys, bad guys
 - No one is just one or the other. People sometime do the right thing, and sometimes not, sometimes knowingly, and sometimes unknowingly.
- Not using risk, or mis-judging risk
 - TSA’s focus on preventing liquids from going through security checkpoints
- “There’s an app for that”
 - Silicon snake oil salesmen, latest APT “mouse trap”, etc.

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Misguided information security thinking

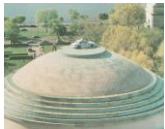


- Saying it is so, will make it so
Compliance is not assured even in organizations where command-control and dictates are used to drive compliance
- Obscurity ≠ security
Kerckhoff's principle – “[a security system] must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience;”

4

Copyright © Scott Bradner & Ben Gaucherin 2016

MIT Hacks



- Student pranks meant to demonstrate technical aptitude, cleverness, creative thinking, etc.
- “An MIT hack is ingenious, benign, and ephemeral mischief pulled off under a cloud of secrecy or misdirection”
Nightwork: A History of Hacks and Pranks at MIT

5

Copyright © Scott Bradner & Ben Gaucherin 2016

The value of “unlearning”



Timothy Kenny



- “Unlearning is the process of dismantling thought structures or belief systems (about how things are) that are not in fact true” – Timothy Kenny
- Industrial design firms focus on un-learning to get to breakthrough ideas/innovations in product design
Nightline - Inside IDEO: Re-examining the Shopping Cart

6

Copyright © Scott Bradner & Ben Gaucherin 2016

Curious minds and strange bedfellows



- *“DEF CON has been an open nexus of hacker culture, a place where seasoned pros, hackers, academics, and feds can meet, share ideas and party on neutral territory. Our community operates in the spirit of openness, verified trust, and mutual respect.”*

- The Dark Tangent



7

Copyright © Scott Bradner & Ben Gaucherin 2016

Curious minds and strange bedfellows



IETF 73 - "graybeards"

8

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide# credit

2 https://commons.wikimedia.org/wiki/File:SmartWater_sign_-_thieves_beware.jpg

3 <http://www.360nobs.com/2014/09/what-do-girls-really-want-bad-guys-or-good-guys/>

3 http://www.nbcnews.com/id/37021555/ns/travel-travel_tips/t/liquid-rules-so-long-/

4 <https://www.linkedin.com/pulse/20140807190144-118550419-pci-non-compliance-the-stick>

4 https://en.wikipedia.org/wiki/Auguste_Kerckhoffs

5 <http://geekslop.com/2012/mit-hacks-pranks-hacker-ethic-influence>

5 <http://wiki.mitadmissions.org/Hacks>

5 <http://www.theverge.com/2012/11/19/3665306/mit-harvard-yale-1982-weather-balloon-prank>

9

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide# credit

6 <http://timothykenny.com/about>

6 <http://www.themplsgeotist.com/news/national/2014/february/23/inside-ideo-re-examining-shopping-cart>

7 <http://lasvegaweekly.com/photos/2012/aug/08/439039/>

7 <http://securityevangelisteu.com/category/information-security/people-associated-with-information-security/>

7 <https://www.youtube.com/watch?v=0gBo16YRjrk>

7 <http://www.zimbio.com/photos/Jeff+Moss/DEFCON+Dark+Tangen+t+2015+Tribeca+Film+Festival/8n4wkuff1yx>


8 <https://americascienceblog.com/2013/09/>

Information Security Strategy, Classification, Policy, and Mindset
Conclusion

CSCI E 45b: The Cyber World – part B

1 Copyright © Scott Bradner & Ben Gaucherin 2016


Final thoughts



- You need the buy-in from the people who need to fund and support information security
Strategy can help with that
- No classification system implies everything gets treated the same: mildly confidential and top secret alike

2 Copyright © Scott Bradner & Ben Gaucherin 2016

Final thoughts



- Without clear and pragmatic policies people are less (or altogether not) likely to behave the way you would like them to
- Even with clear and pragmatic policies people still may not behave the way you would like them to
But at least you can hold them accountable, if you need to

3 Copyright © Scott Bradner & Ben Gaucherin 2016

Final thoughts



- Hackers and security researchers of all kinds have gotten us to where we are today
- Approaching information security through a single lens is at least a missed opportunity, and possibly a mistake
- It takes a village

4

Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

All drawings and photos by Ben Gaucherin unless noted

Slide# credit

2 <http://www.dliffc.edu/faos-professor-discuss-national-security-strategy/>

2 <https://security.harvard.edu>

3 <http://crazyspeechworld.com/2013/03/granny-says-freebie.html>

4 <http://alchetron.com/Moxie-Marlinspike-226394-W>

4 <http://www.reuters.com/article/net-us-usa-security-hackers-idUSBRE86K01U20120721>

4 <http://www.sfchronicle.com/business/article/Hotel-hosting-security-conference-was-the-victim-6791446.php>

5

Copyright © Scott Bradner & Ben Gaucherin 2016
