

Security Awareness at Cal Poly

Ryan Matteson, CISSP

Security Assurance

ITS Office of the CIO

Introduction: My Role

OCIO Security Manager:

To identify security needs and help the campus to meet those needs.

Background: enterprise systems architecture, software development and consulting – CSC, CISSP, SCJP, 10 years at Cal Poly, 10 years Oracle experience, 12 years Unix system administration

Introduction: Your Role(s)

Who are you, why are you here?

Agenda

Topics I will cover:

- What is security? Why does it matter?
- How can we think about security in a productive way?
- How do we become “secure enough”?
- Question and Answer.

What is security?

- Security is freedom from risk or danger.
- Risk can never be completely removed, but it can be lessened.
- Information systems security means: confidentiality, integrity, and availability of information.

Why does it matter?

- At Cal Poly we have many valuable assets, and some of these are held in information systems:
 - Personal information (student, employee, client)
 - Financial information and controls
 - Computational and network resources

Compromises of these assets cost us (time, money, confidence, legal liability, health)

How do we think about security?

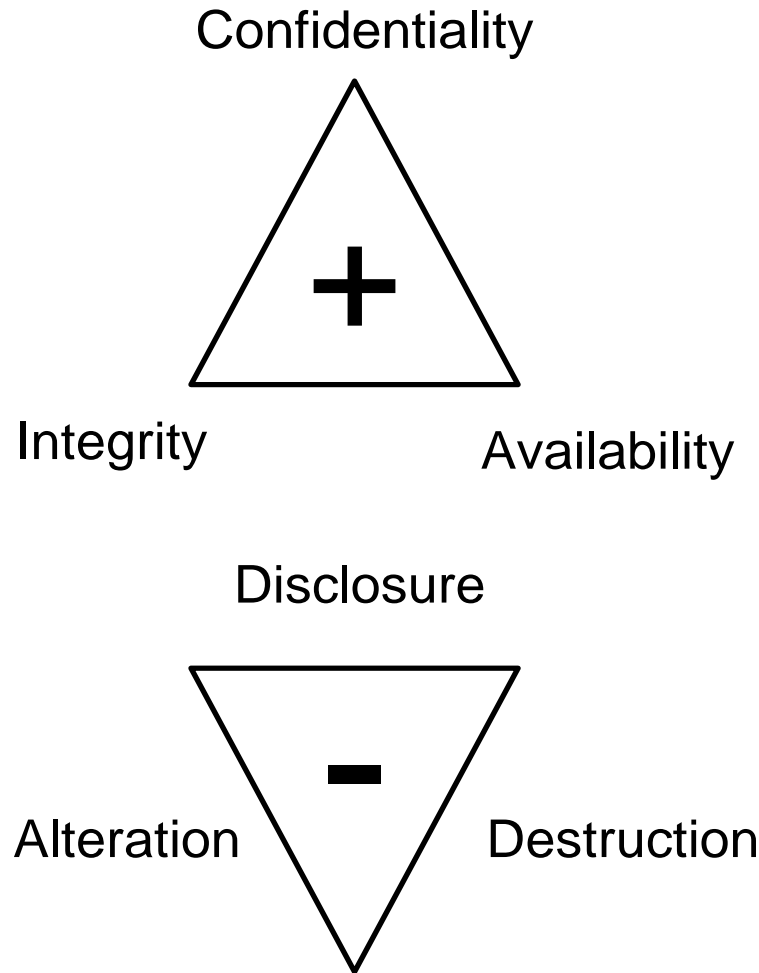
- Security can be:
 - **process**: ongoing effort towards a goal
 - **enabler**: making things practical by lowering risk (it's not about creating inconvenience).
 - **risk management**: allocating resources towards the effort, based on analysis of dangers or costs

All of us share some responsibility for security (for ourselves, for Cal Poly, for the State, ...)

How do we think about security?

- The primary goals are C I A
 - (*not* confusion, ignorance, annoyance!)
- Confidentiality: enforce secrecy
- Integrity: protect accuracy/reliability
- Availability: prevent disruption of service

How do we think about security?

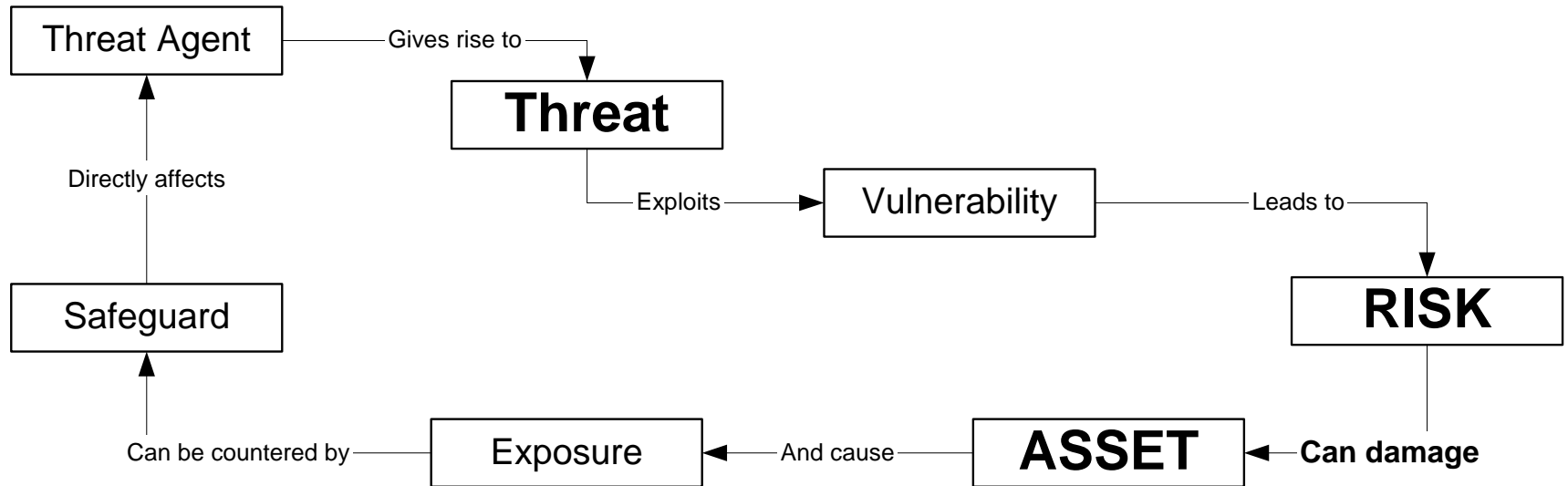


Where should we care **most**?

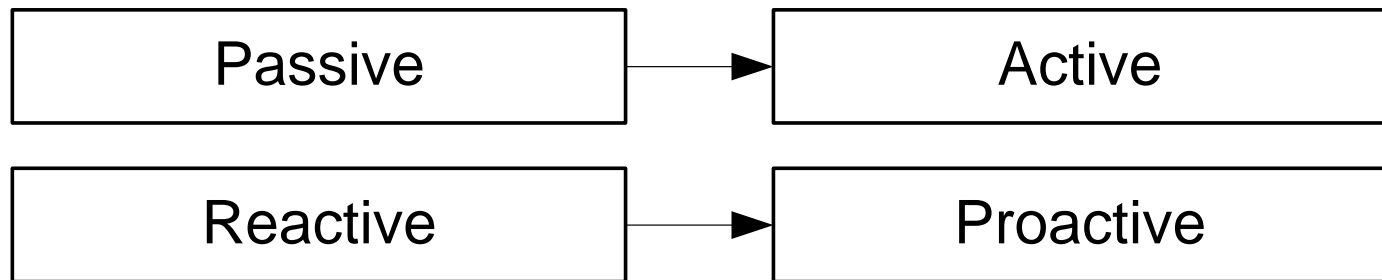
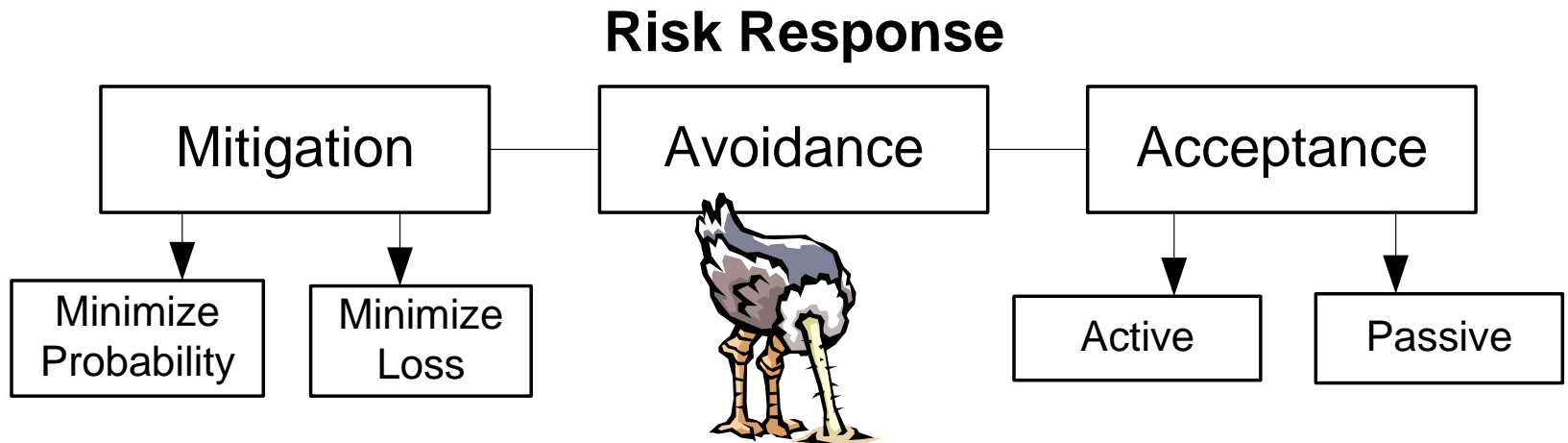
- Where disclosure, alteration, and destruction of data can do the **most harm**.
- Threats to Medical Information:
 - Destruction: very bad
 - Disclosure: extremely bad
 - Alteration: very extremely bad

Liability and danger with any of these.

Risk Management

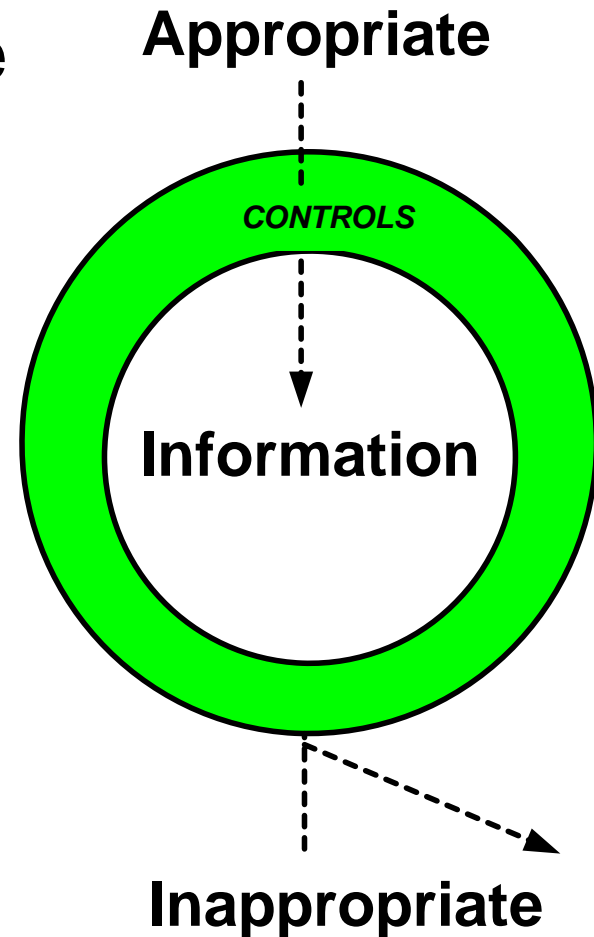


Risk Response



Access Controls

- Mechanisms that direct use of a system: what the user can do, what they can access.
- Help provide all the things we want (C, I, A).
- Common target for attacks.



Access Controls: Password Practices

- Passwords can provide all three (C, I, A)
- To be effective, we must have address the threats that make them less effective.
- Following good password practices is a way for you to help improve security – which benefits you and the University.

How do campus password practices fit in?

- Threats: **guessing**, disclosure, sharing, reuse
 - Passwords must be difficult to guess (including by automated means).
 - Changing them helps too.
 - How ITS is helping: Password Manager at my.calpoly.edu follows rules for passwords that are difficult to guess.

<http://www.alw.nih.gov/Security/Docs/passwd.html>

How do campus password practices fit in?

- Threats: guessing, **disclosure**, sharing, reuse
 - Each user should protect the secrecy of their own password; do not put it on a sticky-note on your monitor!
 - How ITS is helping: single password (used for my.calpoly.edu, e-mail, calendar, PeopleSoft and counting)
 - If you only have one to remember, and you use it often, there's less need to write it down.
 - If you have trouble, call the Service Desk at X67000 or your local support staff – they can help!

How do campus password practices fit in?

- Threats: guessing, disclosure, **sharing**, reuse
 - Intentional disclosure: each user should have and use their own password, and not share it with others.
 - If someone else has a legitimate need to access a system, they should get one through the appropriate process.

How do campus password practices fit in?

- Threats: guessing, disclosure, sharing, **reuse**
 - Reuse: Don't reuse your Cal Poly passwords in other contexts, such as non-University web sites.
 - We have measures in place to keep your password secure when it is used within Cal Poly systems -- but we can't protect it if you share it with xyz.com!
 - Campus, PyraMED, SIS, PPC, workstation.

Getting “secure enough”: shared responsibility

- As employees we have access to sensitive information.
- This comes with a responsibility:
 - confidentiality statement
 - Health and Counseling Services Security Policy
 - University Responsible Use Policy
 - *This list is not complete*

Getting “secure enough”: use the password

- You’ve got a good password
- You’re protecting it
- Benefit from it by
 - Logging off when you’re done (and at least at day end)
 - Locking your computer whenever you step away

Getting “secure enough”: stay within protected systems

- You’ve got a good password
- You’re protecting it
- Benefit from it by
 - Keeping data within systems that restrict access by passwords
 - PyraMED and file servers are good
 - Workstations are less good
 - CD-Rs, ZIP disks, floppies, USB keychains are not good
 - Erase/destroy information that is no longer required (especially on CD-Rs, etc.)

Getting “secure enough”: stay within protected systems

- You’ve got a good locking cabinet
- You’re protecting your keys
- Benefit from it by
 - Keeping paper records in controlled areas
 - Destroying paper that is no longer needed

Getting “secure enough”: keep your system protected

- You’ve got a good password
- You’re protecting it
- But this doesn’t matter if someone else controls your computer!
 - Don’t install non-approved software – it could be doing *anything*
 - Don’t share your access with non-authorized users
 - Work with your LAN coordinator to stay current on protective measures
 - When in doubt, ask!

Review

- Security is important: legal, time, money, confidence.
- Security lets us do *good things*, by preventing *bad things*.
- Passwords help prevent *bad things* – but only when we protect them and utilize them.
- We all share a responsibility.
- There are people who want to help you.

Further learning...

- Health and Counseling Services Security Policy
- Your local technical support staff
- Cal Poly IT Responsible Use Policy
 - <http://www.calpoly.edu/computing/policy.html>
- Password practices
 - http://helpdesk.calpoly.edu/faq/password_faq.html
- Campus Information Security Program
 - <http://its.calpoly.edu/Policies/isp.pdf>
- Beyond Fear
 - “Thinking Sensibly About Security in an Uncertain World”
 - Bruce Schneier, HV6432 .S36 2003

Contacts

- Immediate threats to safety: call 911
- Violations of campus information or responsible use policies:
abuse@calpoly.edu
- Discussion or questions on information security issues: rmatteso@calpoly.edu