**Protecting Information and Resources**

Predict the impact of specific activities on the confidentiality, integrity and availability of personal and university resources and recommend appropriate actions based on those predictions:

* Identify the dimensions of risk to your information and resources: confidentiality, integrity and availability
* Identify risks to the CIA of your personal information and resources
* Describe specific risks to the CIA of university resources that result from common student behaviors
* Identify practices for protecting the CIA of your personal information

*Frank was trying to study, but his roommate’s loud phone conversation was distracting him. “Uhhh-huuuu, yeah, you can do that. Sure, I’ll just give you my password, that way you can put it up on Facebook, and you can also take care of that assignment in the clusters. No, it’s the same password. OK, it’s capital B, zero, capital B, dash, bang. No, bang! It’s an exclamation poi….never mind, I’ll just write it down, it’ll be on my desk for you. OK, thanks—yeah, I’ll see you there. “ As Bob hung up the phone, he noticed Frank’s raised eyebrows, “What?!” “You hand out your password to everybody? Can I have your PIN number too?” Frank asked. Bob shrugged, “No, that was Marijke, it’s ok, I trust her.” Frank shook his head, “Bad idea, man. A friend of mine had a pretty bad breakup last semester. Her ex-boyfriend had her password and he wrecked a lot of her stuff…locked her out of facebook, then made some nasty status updates, changed her university contact info. Oh, a real tragic email to her parents that read like she was on drugs. And I think he might have trashed some research paper she was working on.” Bob shook his head, “Wow, that’s crazy. But Marijke’s ok, I trust her.”*

Whether or not he knows it, Bob’s putting the confidentiality, integrity and accessibility of his personal resources and information at risk; and beyond the risk to himself, he’s also risking some university resources. When thinking about computing security, most of us tend to focus the procedural aspects of identifying and protecting against specific threats—viruses and software updates. These are essential aspects of safe computing, and they’ll be covered later in C@CM. Beyond the mechanics of safe computing, you also have a responsibility for protecting own your information and the information, as well as the information and resources of the university. Although your interests and university’s interests may seem to be quite distinct, in fact there is a relationship to protecting both of them—much as the university has an obligation to keep it’s resources secure (and not release student data), you have a similar obligation to keep your own information secure, and not put the rest of the university community at risk. As you learned earlier in the course, part of this obligation is explicit in the computing policy: [maintain the security and confidentiality of your account](http://www.cmu.edu/policies/documents/Computing.htm).

When considering this responsibility, may students wonder why it’s important; “Who cares if someone gets in my account, it’s just my email” is a fairly common sentiment. In this section of the course, you’ll learn how to answer the question “who cares,” with a careful consideration how to protect your information and resources, including an understanding of what constitutes risk to and compromise of these resources. You’ll then learn how to think about threats to your resources across certain dimensions—Confidentiality, Integrity and Availability (CIA)—and some techniques and best practices for making good decisions about protecting against those threats. Finally, you’ll learn how some of your decisions about protecting information and resources and impact the information and resources of the university community.

**Dimensions of Resource Protection**

Trying to think about information and resource protection can be daunting; simply on the technology side, threats can come from multiple directions, and the types and specifics of these threats are constantly changing—what might have been a safe practice yesterday can become a risky behavior today. Beyond the technology, the human dimension of protection can also be challenging—who can you trust with your information? Who’s a risk? Finally, evaluating what is actually the extent of a risk can be difficulty; the paths between types of information are sometimes fuzzy, and it’s not always obvious that an account like your Andrew ID can access much more than “just your mail”.

And the reality is that it is much more than “just your mail” that you are protecting. Your university credentials can be used to access a broad swath of information—your grades, your financial aid information, even your health records. Beyond simple access, these same credential can be used to modify or change information—your schedule, your contact information, potentially even some pieces of your coursework. It’s also not just your resources; as you learned earlier in the course, many of the university’s resources are shared; your credentials are also a gateway to these communal resources.

Activity: LBD: Just Your Mail?

Using your Andrew id and password, explore resources and information that are available to you with these credentials. Use the portal at <http://my.cmu.edu> as a starting point, but don’t feel constrained to stay within the portal—feel free to look across the cmu.edu domain. After exploring for 10-15 minutes, consider the information or actions below. Using your Andrew credentials, is it possible to:

Find information about your mental health history?

Yes [Correct—this information is part of your general health records]

No [Incorrect—your health records can be viewed using your Andrew credentials]

Add courses to your schedule?

Yes [Correct]

No [Incorrect—via the SIO system, your schedule can be changed]

Remove courses from your schedule?

Yes [Correct—drops are performed using the SIO system]

No [Incorrect—using your credentials, classes can be dropped from your schedule]

Access your bank account?

Yes [Correct—there is no direct access to your bank account]

No [Incorrect—although you can access information about your PlaidCa$h account, there’s no direct bank account link]

Learn about your parent’s income?

Yes [Correct—this is listed in your financial aid information]

No [Incorrect—your parental income is specifically listed in your financial aid application]

Reserve university rooms in your name?

Yes [Correct—space and other resources can be reserved using your credentials]

No [Incorrect—Space quest does allow for resource reservations, sometimes for a fee]

Block you from accessing university services?

Yes [Correct—with your credentials someone can change your password]

No [Incorrect—if someone changes your password without your knowledge, you’ll be unable to access many university services]

**Understanding Risk**

Many people tend to assume that protecting information and resources (whether yours or the university’s) is strictly about large preventative measures such as anti-virus software, firewalls or secure passwords. While these preventative measures are important, they’re also reasonable static, and they don’t easily take into account your everyday actions and activities. Instead of looking only at these preventative measures, we would like to give you a larger framework for evaluating your actions and activities as they relate to resource protection—if you have the ability to evaluate whether an action or activity is particularly risky, and what its consequences might be, you’ll be able to better deal with changes on both the human and technological fronts in an ongoing way.

When we talk about **assessing a risk**, we’re talking about considering an action, activity or general state of affairs in the context of a potential compromise of a resource. Compromise, in the information security sense, may have a slightly different meaning than you are used to:

Definition: Compromise

In the field of information security, a compromise is a breach in the security of a specific resource—potentially a computer, an account, a file or other resource. A resource can be compromised for many reasons, including a malicious attacker “hacking” into a system, but also a well-intentioned user forgetting to log out of a machine.

When performing a risk assessment, then, you’re considering:

1. Is there the possibility of a compromise?
2. How likely is a compromise?
3. If a compromise occurs, how severe are the possible consequences?

Activity: LBD: Assessing Risk

In our introductory scenario, Bob shares his password with his friend Marijke; before sharing a password, a risk assessment is appropriate. In the case of Bob and Marijke, if he shares his password:

 Is there the possibility of a compromise?

Yes [Correct—by definition your credentials is a breach of your security]

No [Incorrect—once you share your password, your resources are no longer protected]

It depends on Bob and Marijke’s relationship [Incorrect—no matter how close the relationship, a compromise has still occurred if an account isn’t secure]

[Hint: If a password is not longer a secret, is it still protecting the resources?]

[Hint: Once the password is insecure, Bob’s account is considered compromised]

Given that sharing his password compromises Bob’s account, how severe are the possible consequences?

Insignificant since Bob trusts Marijke [Incorrect—the possible consequences are independent of Bob and Marijk’s relationship]

Minor [Incorrect—an Andrew id and password can give access to very personal information, and can allow for some fairly dramatic actions]

Major [Correct—although Marijke may not use the password maliciously, it’s still possible for her to use it in ways that can have severe consequences for Bob]

[Hint: Remember that you’re not trying to evaluate how likely consequences are, you are only considering the severity of what’s possible]

**Dimensions of Risk**

Assessing risk, then, involves a consideration how well protected a resource might be, and what the consequences could be if the resource is compromised. Simply asking yourself whether you are doing something that might “put resources at risk” is probably not a useful approach for most people, though. To some extent all actions have a degree of risk—your real goal is to assess that risk in a useful way. And that assessment can be a real challenge—security and risk are complicated and multi-faceted. Because information protection can seem like a large and monolithic problem, security experts break the problem of security into three distinct aspects, considering the Confidentiality, Integrity and Availability of resources, first as discrete pieces and then collectively. By focusing on one specific dimension at a time, you’re able to decompose the question of protection into more manageable parts. And by then considering them collectively, you’re able to make decisions that can best reflect your own priorities and responsibilities.

Definition: Confidentiality
The confidentiality of a resource refers who is able to read or access it. Maintaining the confidentiality of a resource does not require that it be a completely secret or inaccessible; rather it is about ensuring that only authorized users – the right people –have access and that unauthorized users – the wrong people—are excluded.

“A loss of confidentiality is an unauthorized disclosure of information” [[FIPS](http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)]

Example: A Loss of Confidentiality

Morgan is headed to an appointment, and she’s forgotten the room number for her meeting. She calls her roommate, Kayla, and shares her password so that Kayla can login and get the location. After the phone call, Kayla browses through Morgan’s student information and uses financial aid information discover the income level of Morgan’s parents.

Although Morgan authorized Kayla to look up a specific email, she intend to release any information about her parents’ income—the confidentiality of her account has been compromised.

Activity: DIGT

Is password sharing the only way to risk the confidentiality of your computing resources?

Yes [Incorrect—although password sharing is a common example, anything that allows someone unauthorized access to your information breaches your confidentiality]

No [Correct—Any unauthorized access risks the confidentiality of your information; a virus, for example, could open some of your files to other users.]

Definition: Integrity
The Integrity of a resource refers to how trustworthy that resource is. Maintaining the integrity of information means ensuring that the data has not been changed inappropriately, whether these changes are accidental and innocent or are intentional and malicious.

“A loss of integrity is the unauthorized modification or destruction of information.” [[FIPS](http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)]

Example: A Loss of Integrity

Amit headed into the clusters to check his email, and he realized when he sat down that the last student to use the machine—someone with the Andrew ID jstu33—had forgotten to log off. Based on the number of drafts still open on the machine, it also looked like jstu33 had forgotten to save the most current copies of his research. Amit tried to do the right thing and save out the work, but at least two the documents seemed to conflict with files that already existed in jstu33’s directory, so he finally just hit Save All and logged jstu33 out of the machine.

Although some version of jstu33’s research files have been saved, jstu33 can’t be sure if it’s the correct or most recent version of his work; the integrity of his research data has been compromised.

Activity: DIGT

Is it accurate to say that the integrity of a resource is only problematic if you know that information has been modified?

Yes: [Incorrect—Integrity is about your ability to trust that the information is correct; if there is an opportunity for the unauthorized change of a resource, the integrity of that resource is still at risk.

No [Correct—resource integrity can be a problem if there was the possibility of a change; you can only trust the resource if you know that the information was not changed]

Definition: Accessibility

The availability of a resource refers to how timely and reliable access to that resource is. Maintaining the availability of a resource means that authorized users are able to get to the specific machine or information when needed; availability can be threatened for technical reasons (such as a networking problem that prevents access) or more human factors, such as a changed password.

“A loss of availability is the disruption of access to or use of information or an information system.” [[FIPS](http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)]

Example: A Loss of Availability

Xing had set up a linux machine to use for his computer science classes, but he hadn’t bee especially diligent in keeping it up-to-date; this carelessness came back to haunt him when someone used a software vulnerability to access his machine and change the passwords on it. Now Xing can’t log into his own machine and retrieve his assignments.

Because he has physical access to the machine, Xing will eventually be able to get on and get his information, but the process won’t be fast, and during that time he still won’t be able to get to his work; the availability of this resource has been compromised.

Activity: DIGT

Is it accurate to say that the availability of a resource can only be compromised by a malicious attack?

Yes [Incorrect—anything that keeps you from accessing a resource when you need it is an availability problem, no matter how well intentioned].

No [Correct—Well intentioned actions, such as a password change, can still make a resource unavailable]

CITE: [Federal Information Processing Standards (“FIPS”) publication 199](http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)

As you can see, considering how you protect your information and resources using these three dimensions can allow for more focus in evaluating your risks. This focus can help streamline the risk assessment process, and it can also help more clearly identify possible consequences if your resources are compromised.

DIGT: Where is the risk?

In the scenarios below, identify which of the three dimensions is threatened or has been compromised:

Arlina shares her Facebook password with an acquaintance; this acquaintance subsequently changes the password, keeping Arlina from accessing her Facebook account.

Availability

Fred finds his roommate andrew password on a post-it note in their room; he uses the password to:

 snoop on his roommate’s student medical records

Confidentiality

Check out his roommate’s PlaidCa$h balance

Confidentiality

Send joke emails posing as his roommate

Integrity

A computer virus takes over Alfonso’s machine and begins sending thousands of spam emails without his knowledge. The ISO eventually blocks Alfonso’s machine from the network:

Availability

If the virus begin changing Alfonso’s files?

Integrity

If the virus began logging Alfonso’s keyboard and captured the password to his bank website?

Confidentiality

**Multi-dimensionality**

Although we started by talking about considering risks along one specific dimension, the reality is that most threats and compromises can occur across multiple dimensions—sometimes an action can risk two or even three dimensions—for example, sharing your password can lead to a loss of both availability and confidentiality if someone changes your password and looks at your information. Similarly, often a compromise along 1 dimension can lead to a further compromise—having gained access to your account (a confidentiality compromise), an attacker begins changing and deleting files in your AFS space (an integrity compromise).

In practice, this means that you can’t simply assess risk against one of the three axes. Instead you need to consider your actions and obligations across all three dimensions, with a further eye towards how compromises might lead to additional problems.

Activity: Learn By Doing

Returning to some of the examples above, consider these cases—which of the three dimensions are directly threatened or compromised?

Alfonso’s computer is taken over by a computer virus; the virus begins sending out thousands of spam email messages using the contents of Alfonso’s personal files as the mail text?

Confidentiality [Yes, his files are now being exposed both to the virus and anyone it mails

Integrity [No, not directly as written. If the virus began changing or deleting files, the integrity of Alfonso’s data would be threatened]

Availability [Yes, the spam messages can lead to the machine being removed from the Carnegie Mellon network]

After finding his roommate’s Andrew password on a post-it note beside the monitor, Fred uses the password to snoop through his roommate’s email. He also changes a few of his roommate’s homework files, inserting some jokes in among the original text.

Confidentiality [Yes, Fred is using the password to read emails that he’s not authorized to see.]

Integrity [Yes, because Fred changed some his roommate’s homework files, the information is no longer trustworthy.]

Availability [No; although the confidentiality and integrity of the roommate’s account have been compromised, the resources are still available]

**What’s at Stake?**

Although some of the examples that are included above may seem extreme or unlikely, it’s important for you to understand just what is at stake—just what all can be exposed when your university credentials are used? Is there really a danger of your friend or roommate changing your files or information?

Recognize that your Andrew id and password are the key to an exceptional amount of personal information. With regard to confidentiality, for example, someone with your credentials can see:

* Your e-mail.
* Your schedule of classes.
* All of your contact information
* All of your academic records, including your grades
* Your medical records—this includes both your physical and mental health history.
* Your financial aid information; remember that your financial aid application doesn’t list only your information, it also includes detailed information about your parents occupations and income.

In addition to information that most students would consider confidential, your Andrew credentials also give the ability to change information, including:

* Your contact information
* Your home mailing address
* Your class schedule, including dropping and adding classes
* Any files that you’ve stored on the university network
* Your faculty course evaluations
* Your network registration information

Finally, using your Andrew credentials, someone can place severe limits on the availability of some of your resources:

* Changing your password
* Deleting your files
* Removing your computer from the network
* Getting your account suspended from the network.

It’s important for you to understand that these possibilities are not just theoretical; all of the bullets above represent actual resource compromises that not only can be threatened or changed but that actual students have had occur. Sometimes these compromises have been the result of malicious actions, but just as often they’ve occurred by mistake or as an intended prank.

**Best and Worst Practices**

Actually walking through and literally pre-considering every possible threat to your information and resources is probably not realistic for most of us. It’s hard (and sometimes impossible) to predict the long-term outcomes for every action we might take. And even if we’re capable of doing that kind of long-term consideration, most of us simply don’t have the time to commit to it.

Rather than trying to analyze every action, it’s helpful to rely on some general rules-of-thumb for best (and worst) practices when protecting information and resources. The safe computing section of the course will give you more information on procedures and practices for protecting yourself and your resources from harm. In terms of generally living up to your responsibilities for protecting your information and resources, however, the following best practices are useful:

* Keep your passwords to yourself
Although there are many potential paths and vectors for compromising the CIA of your resources, the vast majority of cases can be avoided simply by maintaining a secure password and not sharing it. Indeed, this one rule is so important that it’s been codified as an explicit responsibility in the university computing policy.
* Use different passwords for different accounts.
Remembering multiple passwords can be a challenge, and it’s often convenient to use the same password for multiple accounts, ranging from Facebook and your bank account to your Andrew id and twitter page. The danger here is that a compromise on any one of these accounts also compromises all of the others. Are you willing to trust your bank account information to the security measures that Flickr has put in place?
* Use secure passwords
Although the university now uses technology to force you set and maintain a secure password for your Andrew credentials, it’s worth remembering that most other sites and resources do not. When selecting a password, the university [password requirements](http://www.cmu.edu/computing/accounts/passwords/requirements.html) are still good guidelines. And if you find it difficult to remember so many secure passwords, don’t just jot them down on a piece of paper; instead consider [encrypting](http://www.cmu.edu/computing/doc/security/encrypt/index.html) them.
* Think about longer-term consequences
Although it’s impossible to accurately predict every long-term outcome for any action that you take, that doesn’t mean that it’s not worth considering what some non-immediate consequences can be. Remember just how much of your information and resources are interconnected, and just how much can be exposed with one set of credentials.
* Remember that people are the [weakest link in security](http://www.google.com/search?client=safari&rls=en&q=people+weakest+link+security&ie=UTF-8&oe=UTF-8)
No matter how secure you make your passwords and how careful you are with your technology, there is always a human element to protecting your information. You’ll learn more about how easy it is for people to make mistakes in protecting their information later in this course—especially with regard to phishing and social engineering threats; for now, simply recognize that you need to treat your information with care. And further, remember that even people that you trust can make mistakes—if you’re the weakest link in protecting your own personal information, how much more effective can you expect your friends to be in protecting it for you.
* Log out
Whether it’s your personal machine or a cluster computer, always remember to log out when you leave the machine. This one may seem obvious, but students consistently forget to log out of the clusters, leaving their Andrew identity wide open for the next student that sits down. Most of the time this doesn’t lead to problems and the next user will just log the forgetful student out, but each year some issues do arise. Similarly, make a practice of logging out of your personal machine as well, especially when you’re not with it; if it’s not possible to control who has physical access to your machine, then be sure to control who has access to the data that’s on it.

Activity? LBD

*I think this section needs some kind of activity for students to apply these rules of thumb, but I’m not sure how to craft one that’s not stupidly simple. I’m also not convinced I have the rules of thumb correct. Help from ISO team? Or could this be a submit and compare?*

*Activity: DIGT: Protecting Your Personal Information*

*This activity also needs to be developed. Some kind of culminative set of questions that puts all of this together. I’m thinking three scenarios where a student is about to or has already, do something. In each case students need to evaluate what’s at risk (CIA) (probably along a 1-3 scale), and then give a suggested action (choose from a list). The challenge here is not just using “don’t give out your password” scenarios. Some possibilities:*

1. *Giving friend facebook password. Password is similar to Andrew ID. At risk: Conf (a little) Avail (if she changes it). Actions: don’t give out password, make passwords more dissimilar, don’t be paranoid, ?*
2. *Classmate is in a hurry to get file off of you’re my file, asks for password. Work due very soon…(Conf, Avail, Integrity all at risk), Actions (send file, use CMU-provided sharing mechanisms, login yourself and then let them navigate, ?)*
3. *More…*

**Why Protection is a Responsibility**

Throughout this section of the course, we’ve talked about your responsibility to protect your information and resources. Given that most of the examples and scenarios that we’ve described seem to focus on personal consequences, it may seem reasonable to think of this as strictly a personal issue. If there’s no one but yourself that can be affected by your actions, why does the course spend this much time on the topic? And why is this specific issue directly addressed in the computing policy?

The answer is that although the largest threat is to your own personal information, there are consequences beyond your own personal embarrassment, discomfort or inconvenience. As we’ve already noted, within the information that can be accessed using your Andrew credentials are some pieces of data that others might want confidential—your parents contact and financial information, to use one example.

Beyond the confidentiality of others’ information, there’s also the larger question of how your resources and information relate to the larger community’s. Significant parts of the university rely on the assumption that the integrity of student information can be trusted. If even simple information like student contact information can’t be assumed to be accurate, systems ranging from university billing to emergency alert systems do not work nearly as well.

There’s also a cost involved to cleaning up after a personal compromise, and this is a cost that’s borne by the university as much as it is by you. Although much of the time commitment and direct financial costs from compromises are yours alone, there’s also a cost to the university. Carnegie Mellon personnel need to spend time investigating security breaches, resetting passwords and verifying information in the event of a compromise, and this represents a real cost—one that’s paid for from tuition dollars.

Finally, it’s important to recognize that just as your personal behaviors can risk the CIA of your personal resources, they can also threaten the CIA of the larger university’s resources. Carnegie Mellon’s resources are often a target of malicious attacks, for reasons ranging from the speed of its networks to the vast amount of personal data that they contain. Although your credentials may not be able to provide direct access to this all of this information and resource, once they are compromised a malicious attacker is one step closer to compromising other community resources. Although the university takes significant steps to isolate its resources from the potential misdeeds of individual students, the reality is that university computing resources are shared by the community; as a member of the community you have a responsibility to protect them.

Activity: LBD: In the following examples, identify which dimension has been place at risk by student behavior: university confidentiality, integrity or accessibility:

1 Student shares password; as a joke, friend changes contact information to the white house. (I)

2 Social networking site compromised; attacker gains access to university network and begins snooping on network traffic. (C)

3 Virus takes over student machine, launched DDOS against other university resources (A)

Are there more/better examples?

Still Needed:

DIGT on protection as responsibility

Many Students Wonder: Special Responsibilities for Student Workers

Summary

To Learn More:

* [The Information Security Office](http://www.cmu.edu/iso/)
* [College Students: Staying Safe Online](http://www.staysafeonline.org/content/for-students)
* Others?